КИБЕРНЕТИКА

Ю. И. МАНИН

ВЫЧИСЛИМОЕ И НЕВЫЧИСЛИМОЕ

Настоящая серия печатается по рекомендации IX Международного Совещания руководителей научно-технических издательств социалистических стран (июнь 1975). В серии участвуют:

Издательство «Советское радио» (СССР)
Издательство технической литературы (ВНР)
Издательство «Техника» (ГДР)
Издательство научно-технической литературы (ЧССР)

● КИБЕРНЕТИКА ●

Ю. И. МАНИН

ВЫЧИСЛИМОЕ И НЕВЫЧИСЛИМОЕ

Москва «Советское радио» 1980

ББК 32.81.
М23
УДК 51—007

Манин Ю. И.

М23 Вычислимое и невычислимое. — М.: Сов. радио, 1980. — 128 с., ил. (Кибернетика).

45 к.

Книга посвящена доказательству существования невычислимых функций и алгоритмически неразрешимых задач. Обсуждаются проблемы оценки сложности вычислений и алгоритмов.

Книга будет полезна широкому кругу специалистов, занимающихся проблемами машинного перевода, искусственного интеллекта, общего использования ЭВМ.

М $\frac{30501\text{-}072}{046(01)\text{-}80}$ 68-81 2500000000 32.81
6Ф0.1

Рецензенты: чл.-корр. АПН СССР *В. П. Зинченко*,
док. физ.-мат. наук *И. М. Яглом*.

Редакция кибернетической литературы

ПРЕДИСЛОВИЕ

Использование электронно-вычислительной техники связано с возможностью алгоритмического решения задач и эффективного вычисления функций. Между тем в математике широко используются функции, заданные неэффективными определениями. Столь же часты доказательства разрешимости задач, например оптимизации, не сопровождаемые алгоритмами их решения.

В действительности класс задач, доступных классическим средствам, в некотором трудно уточняемом смысле строго шире класса задач, решаемых алгоритмически. Книга посвящена прояснению смысла этого утверждения, изложению математических моделей вычислимости, а также некоторых недавних результатов, которые используют понятия теории вычислимости, но выходят за ее пределы. Сюда относятся прежде всего идеи А. Н. Колмогорова о связях понятий вычислимости и случайности, а также результаты о теоретико-числовых аспектах теории вычислений. Более подробно математическая проблематика книги обсуждена во введении.

Скажем несколько слов о том, как книгу можно читать. Прежде всего, для понимания большей ее части достаточно минимальных математических знаний, но, конечно, необходима некоторая математическая культура. Ее характер примерно определяется соединением привычки к теоретико-множественным понятиям начального анализа (функции, их графики, области определения) и навыков составления простых программ. Основные понятия, приводимые в книге (рекурсивная функция, перечислимое множество, алгоритмическая разрешимость массовой задачи и др.), важнее, чем доказываемые о них теоремы, а формулировки теорем важнее, чем их доказательства. Хотя в конечном счете овладение понятиями идет и через проработку доказательств, знакомство с последними может надолго остаться поверхностным. Местами в доказательствах нужны технические сведения из алгебры и теории чисел; все такие места и вообще «кухня» выделены петитом.

Глава I книги содержит большую часть основных определений, они тут же подробно прокомментированы. Читая эту главу, можно опустить доказательства в § 4 и 5. Во второй главе по существу доказывается одна теорема. Рекомендуется продумать ее формулировку, данную в § 1, доказательства снова можно пропустить. Эта теорема и рассуждение из гл. III дают некоторый универсальный способ опи-

сания любой вычислимой функции, требующий только вычисления значений одного (!) универсального полинома и перебора. Этот результат имеет важное принципиальное значение и используется во всех последующих главах, но его доказательство не используется вовсе.

Главы III, IV и V вместе, VI посвящены отдельным темам и могут читаться независимо, сразу после второй главы. Последняя глава вообще заметно более специальна и может быть опущена при чтении. В ней изложена очень знаменитая и трудная теорема теории групп. Подробнее о содержании остальных глав см. во введении.

Различным аспектам теории вычислимости посвящена обширная литература. Читатель, впервые знакомящийся с ней и не желающий вникать в математику, получит удовольствие и пользу из популярных работ В. А. Успенского [9] и Н. А. Криницкого [8]. Учебники по теории рекурсивных функций, рассчитанные на профессиональных математиков, — это книги В. А. Успенского [1], Х. Роджерса [2] и А. И. Мальцева [3]. Монография А. А. Маркова [4] подробно излагает созданный автором подход к теории алгоритмов, основанный на идее о том, что первичные понятия должны формализовать элементарные процессы обработки линейных символьных текстов. Теория машин Тьюринга, популярная альтернативная модель вычислимости, описана в сборнике [7]. Увлекательная книга А. П. Ершова [11] дает живое представление о том, как развивается сейчас теория программирования, не отделимая от запросов практики и возможностей ближайшего поколения компьютеров. По поводу тем, кратко затронутых во введении, см. две замечательные статьи А. Н. Колмогорова [19, 20], написанные весьма неформально. Мы совсем не касались в книге задач построения конкретных экономных алгоритмов. Книга [32] — одна из последних сводок на эту тему. Почти все нужные теоретико-числовые сведения можно подчерпнуть из книги М. М. Постникова [31]. Остальная литература из списка по тем или иным поводам цитируется в книге.

В заключение я хотел бы поблагодарить И. М. Яглома и В. П. Зинченко за внимательное и доброжелательное рецензирование рукописи.

Ю. И. Манин

ВВЕДЕНИЕ

1. Алгоритм — это текст, который в определенных обстоятельствах может привести к однозначному развитию событий — процессу выполнения алгоритма. Фермент, катализирующий специфическую реакцию, устав караульной службы или программа ЭВМ — примеры алгоритмов в этом широком смысле слова.

Математика поставляет алгоритмы вычислений и обработки символьной информации, которые являются существенными компонентами научной деятельности; языки для записи алгоритмов, их работы и результатов; проекты физических устройств, выполняющих алгоритмы. Наконец, математика строит теоретические модели всех этих понятий.

Таким теоретическим моделям — математической теории алгоритмической вычислимости — посвящена эта книга. Она является естественным продолжением книги «Доказуемое и недоказуемое» (М.: Сов. радио, 1979; ниже цитируется как «Д и НД»), но по большей части может быть прочитана независимо от нее.

2. Простейшая, но очень универсальная модель алгоритма постулирует, что алгоритм предписывает способ вычисления функции, заданной на подмножестве целых положительных чисел Z^+ и принимающей целые положительные значения. Для одной и той же функции таких способов может быть много. Оказывается, что среди них есть следующий типовой способ: по любому описанию алгоритма вычисления функции $y = f(x)$ можно построить многочлен

$$P_f(x, y; t_1, \ldots, t_n)$$

с целыми коэффициентами, такой, что $b = f(a)$, если и только если существуют целые числа $t_1^0, \ldots, t_n^0 \in Z^+$ с условием

$$P_f(a, b; t_1^0, \ldots, t_n^0) = 0.$$

Зная P_f и a, мы можем найти $b = f(a)$ перебором векторов $(b, t_1, \ldots, t_n)$ по очереди. Это — основной результат первых двух глав книги. Путь к нему долог. Первая половина пути состоит в анализе самой идеи детерминированного процесса вычислений; этот анализ приводит к представлению о том, что такой процесс может быть разложен на элементарные шаги из конечного и фиксированного раз и навсегда списка и что функции, вычислимые с помощью итерации этих шагов, исчерпывают функции, вычислимые любым другим алго-

ритмическим способом. Последнее утверждение является естественнонаучным постулатом, который не доказывается математически, но подтверждается экспериментально. Такой анализ связан с именами Тьюринга, Черча, Поста, Маркова, Клини, Колмогорова. Он приводит к математическому определению рекурсивной функции, которое вводится и изучается в первой главе.

Вторая половина пути состоит в математической обработке понятия рекурсивной функции средствами элементарной, но очень нетривиальной теории чисел. Первые идеи здесь были заложены в работах Геделя, Дэйвиса, Патнэма, Дж. Робинсон, а завершающий результат получен Ю. В. Матиясевичем.

3. Реальный процесс вычислений производится над *записями* чисел, скажем, в двоичной системе. Первый этап работы любой большой ЭВМ состоит в алгоритмической переработке программы, написанной на языке программирования, в программу на языке машинных команд. Осуществляющий такую переработку транслятор есть алгоритм, переводящий символьную информацию в символьную. Поэтому в математической теории вычислимости, опирающейся на понятие рекурсивной функции, должна найти свое место модель связи между числами и текстами. Такой модели — нумерации Геделя — посвящена гл. IV. Ее основной результат состоит в том, что все элементарные операции над текстом, которые могут лечь в основу процессов алгоритмической переработки текстов, превращаются в рекурсивные функции при любой естественной нумерации текстов. Поэтому нумерация позволяет перевести такую теорию на язык рекурсивных функций.

Принципиальное значение этого результата состоит в том, что он открывает возможности вводить разного рода «замыкания вычислительного универсума». Если аргументы и значения вычислимых функций могут быть текстами, то текст, описывающий алгоритм, сам может быть предметом обработки алгоритмом. Далее можно вообразить себе алгоритм, порождающий все тексты, которые являются описаниями алгоритмов.

Исследование свойств таких универсальных конструкций, в частности эффектов самоприменимости, приводит к обнаружению алгоритмически неразрешимых математических задач и недоказуемых теорем в формальных языках. Очень общему результату Геделя о неполноте формальной математики посвящена пятая глава, а одной тонкой неразрешимой задаче из теории групп — шестая глава.

Теорема Матиясевича из гл. II также немедленно приводит к утверждению о неразрешимости одной из знаменитых проблем Гильберта.

4. Существование алгоритмически неразрешимых задач и формально недоказуемых истин было первым фундаментальным открытием теории вычислимости, если не считать самой системы основных понятий этой теории. Сейчас такого рода результаты продолжают

появляться и вызывать интерес: см., например, § 6 гл V, где сформулирована усиленная теорема Рамсея — несложное комбинированное утверждение, невыводимость которого из аксиом арифметики была обнаружена лишь в 1977 году. Но основные тенденции теории вычислимости определяются работами, которые мотивированы ее прикладными, общематематическими и даже общенаучными аспектами.

К первому направлению относятся многочисленные работы по созданию эффективных, т. е. укладывающихся в реальные ограничения на время работы и объем памяти, алгоритмов решения конкретных вычислительных задач и теории алгоритмов. Сюда же относятся разработки языков программирования и трансляторов, а также принципов их создания. Возникающая новая дисциплина — теоретическое программирование — вынуждена при этом работать иногда на самом краю «пропасти неразрешимости», но все же ее главная забота состоит в том, как сделать хорошо то, что в принципе сделать можно. Цели и объем этой книги не позволили нам коснуться этой огромной и важной области Теория рекурсивных функций лишь очерчивает ее самые отдаленные границы.

Ко второму направлению можно отнести исследования, связывающие теорию вычислимости с более классическими математическими структурами. Так же, как соединение структур группы и дифференцируемого многообразия приводит к понятию группы Ли, ко многим математическим определениям можно добавить условие вычислимости входящих в это определение операций или, более общо, конструктивности объектов и получить новую версию традиционной теории. Уже построены конструктивные варианты анализа из фрагментов других теорий. Можно надеяться, что предрассудки философского порядка, связывающие эти идеи с устаревшими концепциями «обоснования математики», будут постепенно отходить в тень и общематематическая роль полученных результатов будет осознаваться яснее. Конструктивная математика призвана не заменить классическую, а стать ее полноправной частью. В частности, задача характеризации рекурсивных структур в более обычных терминах, образцами которой служат теоремы Матиясевича (гл. II) и Хигмэна (гл. VI), вероятно, даст еще много замечательных результатов. Пример гораздо менее прямолинейной связи рекурсивности с классической математикой представляют глубокие идеи А. Н. Колмогорова в теории сложности и теории вероятностей, введению в которые посвящена гл. III. Формально говоря, одна из задач, решенных Колмогоровым и его учениками, состоит в точной математической характеризации случайных последовательностей. Но по существу Колмогоров сделал предметом глубокой теории интуитивное ощущение того, что степень организованности больших структур (в противовес их случайности и хаотичности) проявляется в ходе алгоритмического взаимодействия с ними, далеко не сводящегося к простым процедурам подсчета частот (см. § 3 гл. III).

Поэтому теорию Колмогорова [19—21] можно с равным правом отнести к третьему направлению развития идей вычислимости, направлению, где теория алгоритмов рассматривается как формализованная модель алгоритмической деятельности и алгоритмических процессов в широком понимании. К таким процессам относится, скажем, перевод текстов на естественных языках или разворачивание генотипа в фенотип, происходящее в процессе развития живого организма.

Такая точка зрения на алгоритмы позволяет увидеть неожиданные аналогии и постановки задач, заслуживающие обдумывания. Опишем вкратце два круга идей, относящихся к лингвистике и физике соответственно.

5. Язык в широком плане есть структура управляющих воздействий в сложной системе; речь — конкретный фрагмент таких воздействий. Соотношение *текст /значение текста* подобно не соотношению *фотография / реальность*, *а* соотношению *программа / выдача* или *программа / вычислительный процесс*.

В результате многолетней работы над проблемой автоматического перевода выкристаллизовалась одна из значительных общих концепций современной лингвистики: известная модель «смысл ↔ текст» (см. [14, 15]). В этой модели язык представляется как соответствие между двумя бесконечными множествами: *«текстов»* и *«смыслов»*. Элементами первого множества являются тексты на том или ином естественном языке; элементами второго — также тексты, но на искусственном семантическом языке, подлежащем конструированию. Соответствие сопоставляет каждый естественный текст с набором его возможных смыслов, а каждый смысл — с набором его возможных выражений на естественном языке. Семантический язык в принципе должен быть универсальным по разным параметрам, в частности, не зависящим от исходного естественного языка. Лингвистика есть теория перевода «смысл ↔ текст». Перевод должен осуществляться через ряд промежуточных этапов, называемых уровнями представления предложений естественного языка. К этим уровням относятся: фонетический (или орфографический), фонологический, поверхностно-морфологический, глубинно-морфологический, поверхностно-синтаксический, глубинно-синтаксический и семантический. «Каждый из уровней, за исключением, может быть, орфографического, задается своим формальным языком; на каждом из уровней исходное предложение имеет формальный образ, называемый представлением предложения — фонологическим, поверхностно-морфологическим, глубинно-морфологическим и т. д.» [15, с. 4].

«Модель «смысл ↔ текст», таким образом, является инструментом, который делает возможным овладение смыслом большого круга текстов на естественном языке. Поэтому представляется заманчивой реализация этой модели на ЭВМ и ее использование для решения за-

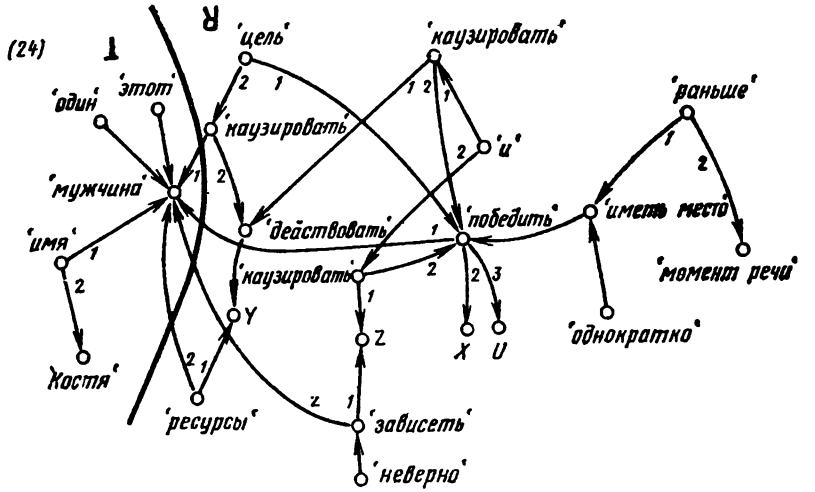

Рис. 1

дач, возникающих в различных автоматических и автоматизированных системах обработки текстовой информации» [15, с. 5].

Разработка детализированной модели — долгое и кропотливое дело. Анализ даже простых образцов бытовой речи приводит к довольно сложным комбинаторным структурам на уровне семантического представления (см. рис. 1, где приведено семантическое представление фразы «Косте удалось победить», взятое из [14; с. 67]). В исследовании оказываются запутанными проблемы анализа семантики и создания языка смыслов и собственно перевода в обе стороны. Неясно, какой максимальный уровень структурированности может быть достигнут и каково происхождение «неалгоритмизуемого остатка»: является ли он следствием исторических случайностей и прихотливости естественного языка или есть более глубокие причины его существования

Некоторый свет на этот вопрос проливает попытка рассмотреть упрощенные варианты описанной программы как бы модели «смысл ↔ ↔ текст». В частности, удобно выбрать такую ограниченную область смыслов, чтобы ее семантическое представление имело возможно более простую и фиксированную структуру. Выберем в качестве этой области «натуральные числа», семантически представляя их последовательностями палочек: I, II, III, IIII, ..., История ее представления средствами естественных языков относится к описательной лингвистике; одновременно она доставляет ценные свидетельства о ранних стадиях математического мышления.

В частности, «предматематический» период отражен в следующих чертах системы названий чисел в различных естественных языках.

В некоторых примитивных языках имеются названия лишь для малых натуральных чисел, остальные обозначаются единым словом «много». Так, в папуасских языках Генде, Кати, Каморо имеется два собственно числительных 1 и 2, далее до 20 счет идет по пальцам рук и ног, на 20 натуральный ряд «кончается». Разумеется, система {1, ..., 20, много} может быть без труда оформлена как непротиворечивый «малый универсум» математики. Более того, такой и аналогичные натуральные ряды заново рассматриваются в одной из школ оснований математики («ультраинтуиционизм») на равных или даже преимущественных правах со стандартным натуральным рядом классической математики. Однако нельзя переоценивать значения этого рафинированного возвращения сознания к архаичным стадиям и отказываться от могущественной идеи потенциально или даже актуально бесконечной продолжимости ряда целых чисел.

В некоторых языках сохранились разные серии названий числительных для счета предметов разной природы (длинных, круглых, одушевленных, неодушевленных и т. п.). Это свидетельствует о долгом периоде формирования идеи о числе как об инструменте, пригодном для счета «чего угодно». Сознание человека довольно долго не было готово к объединению в один «класс эквивалентности» произвольных (хотя бы и малых конечных) равномощных множеств; эта же идея в применении к бесконечным множествам стала достоянием математики лишь после работ Г. Кантора. Следы таких разных типов счета сохранились в современном китайском языке, где хотя и имеется единая система числительных, но она дополняется развитой системой счетных частиц, употребляемых с существительными разных классов типа kuài («кусок»), ge («штука»), ben («корешок») и т. д.

В ряде языков отмечается различие корней, от которых образуются соответствующие порядковые и количественные числительные (ср. uno/primo, duo/secundo в латыни). В этих свидетельствах можно усмотреть весьма раннее зарождение идеи порядка (в отличие от идеи количества), оформившейся в качестве самостоятельного математического понятия удивительно поздно («кардиналы» и «ординалы» Кантора и структуры порядка Н. Бурбаки).

Первые дошедшие до нас тексты (Вавилон, Египет) отражают уже картину развитых математических знаний, в частности, зарождение языка математических обозначений, достаточно четко отдаленного от естественного языка. Основное место в нем занимает система обозначений чисел и операций над ними. Предыстория позиционной системы обозначений современного типа основана на идее счета все более крупными единицами. Эти единицы могут быть степенями одного и того же числа (основание позиционной системы), но это не обязательно. Так, в хронологической системе майев единицы счета суть 1, 18, 360 и далее 18, 20 (ср. следы архаического счета двадцатками во французских числительных типа quatrevingt six) Число единиц очередного разряда обозначается специальным символом, который в начале

может зависеть и от номера разряда (у египтян, греков, римлян). Когда этот символ перестает зависеть от номера разряда и последний определяется лишь положением символа в цепочке, для недвусмысленного прочтения записи становится необходимым символ нуля. Его появление задерживается довольно надолго; к концу вавилонской традиции отсутствие единиц данного разряда отличается нулем лишь в середине записи. Идея о том, что символ нуля является не просто значком, но обозначением самостоятельного числа, имеет еще более позднее происхождение и приписывается индусам, у которых она была заимствована европейской математикой под арабским влиянием. Сама позиционная запись содержит уже зачатки теории алгебраических операций над числами: прочтение записи требует умножения единицы очередного разряда на число этих единиц и сложения результатов. Правила выполнения действий над целыми числами в позиционной записи были даны аль-Хорезми*), имя которого фонетически трансформировалось в современное слово алгоритм.

На этом уровне система названий чисел в естественном языке перестает быть лингвистическим материалом: «тысяча девятьсот восемьдесят четыре» есть собственно название десятичной записи 1984, а не числа, изображаемого этой записью, т. е. некоторое вторичное явление. (Число 1000 в двоичной записи психологически трудно прочесть, «восемь» воспринимается сейчас скорее как имя *цифры*, чем имя *числа*.) Поэтому откажемся от рассмотрения наименований чисел в естественном языке и попытаемся представить себе характерные черты любой мыслимой системы наименований: десятичной, двоичной или даже не обязательно позиционной. Очевидно, минимальные требования должны быть такими: наименования должны быть конечными текстами; способ восстановления числа по наименованию должен быть вычислимой функцией, т. е. задаваться алгоритмом. Если бы дело этим ограничивалось, нечего было бы заменять наименования I, II, III, ... другими. Позиционная система реализует фундаментальное открытие: число N можно записать $\sim \log N$ знаками вместо палочек: даже очень большие числа имеют короткие записи. Смысл записи воплощен в алгоритме ее переработки в последовательность палочек. Правила аль-Хорезми суть алгоритмы переработки записи двух чисел в записи их суммы и произведения.

Но тогда в качестве модели системы наименований чисел мы можем взять любую вычислимую функцию f от натуральных чисел (вспомним, что тексты можно заменять их номерами Геделя , принимающую все натуральные значения. Оставив в стороне вычислимость операций, сосредоточимая. на идее экономии: нас интересует функция f, такая, чтобы имя n каждого числа N, т. е. значение аргумента f, для которого

*) Хорезми, Мухаммед бен Муса — узб. математик и астроном IX в. Автор арифметического трактата, алгебраического труда «Книга о восстановлении и противопоставлении» и др. (*Прим. ред.*)

$f(n) = N$, было настолько малым, насколько это вообще возможно (в двоичной записи числа «$10^{10^{\cdot^{\cdot^{\cdot^{10}}}}}$ (1000 раз)» очень много бит, но мы сумели записать его совсем коротко. См. также сведения о функции Рамсея в § 6 гл. V). Как доказал А. Н. Колмогоров, такие функции f существуют и могут быть построены явно: каждая из них позволяет назвать число N настолько коротким именем, насколько позволяет любая другая система наименований g, возможно, с потерей некоторого числа бит, зависящего от f и g, но не от N.

Однако это условие оптимальности неизбежно влечет за собой следующие свойства функции f. В любой оптимальной системе наименований

а) *Каждое число имеет бесконечно много наименований.*

б) *Не все целые числа n являются наименованиями: функция f лишь частично рекурсивна, но не общерекурсивна, и не может быть продолжена до общерекурсивной.*

в) *Восстановление числа по его наименованию в оптимальной системе требует работы сложного алгоритма: оптимальные функции строятся с помощью универсальных вычислимых функций, которые в некотором смысле настолько сложны, насколько это вообще возможно.*

г) *Проблема отыскания по числу его наиболее короткого наименования алгоритмически неразрешима: анализ большого числа на предмет обнаружения структурированности, позволяющей назвать его коротко, есть творческая задача.*

Сопоставим этот список свойств оптимальной системы наименований чисел со следующими свойствами естественного языка:

А. *Обилие синонимии: каждый смысл может быть выражен огромным количеством текстов на естественном языке.* (Для фразы «Смит не сумел перевести этот текст только из-за того, что в нем оказалось много специальных терминов» по оценке [14] имеется более миллиона перефразировок.)

Б. *Открытость языка: на каждый момент времени не все грамматически правильные тексты осмыслены.* (Эта краткая констатация нуждается в тщательном обсуждении. В модели «Смысл ↔ Текст» полагается, что любой правильный текст может быть переведен в правильный текст на языке смыслов, но среди последних есть «бессмысленные» в неформальном понимании этого слова: интересующая нас категория, стало быть, переводится на другой уровень.) Эта открытость естественного языка является исключительно важным резервом его творческого использования не только в поэзии и философии, но и в науке. Для выражения вновь возникающего смысла может быть использован ранее неосмысленный текст («волна вероятности» в квантовой механике или более прозаический «пакет молока». Еще интереснее факты рождения нового смысла из ранее неосмысляемых, хотя и грамматически допустимых языковых выражений (поэтические метафоры; континуальные интегралы Фейнмана).

В. *Перевод «Текст ↔ Смысл» требует многоступенчатой работы системы сложных алгоритмов, выявляющих огромную структурированность языковых конструкций.*

Г. *Во всех разработках перевод «Смысл ↔ Текст» оказывается еще гораздо более трудным, чем обратный.*

Сопоставление свойств а) — г) и А. — Г. показывает их удивительный параллелизм. Это побуждает высказать гипотезу о том, что многие черты естественных языков, обычно относимые за счет исторических случайностей, хотя бы частично отражают свойства экономичности языка: его возможности кратко выразить сложный смысл, который такое выражение вообще допускает. Обилие синонимических способов выражения и бессмысленных текстов кажется противоречащим этой гипотезе, но если считать нашу модель адекватной, то это обилие парадоксальным образом оказывается неизбежным следствием экономичности.

6. В посленьютоновской физике основным выражением идеи детерминированности служит принцип, согласно которому развитие изолированной физической системы в пространстве — времени определяется дифференциальными уравнениями («законы природы») и граничиыми (начальными) условиями. Этот принцип принимается и в квантовой идеологии: вероятностный аспект квантовой теории существен для описания взаимодействий, в частности, с измерительным устройством, но не для теории изолированной системы.

Вычислительный процесс можно рассматривать как другую модель идеи детерминированности. Она во многом параллельна первой: «закон» отвечает структуре вычислительного устройства, начальные условия — программам. Разбиение вычислительного процесса на элементарные шаги, включающие, в частности, простейшие малые изменения содержимого памяти (как стирание или вписывание символа на ленте машины Тьюринга), можно сопоставить с идеей дифференцирования. В таких процедурах, как решение уравнения теплопроводности методом сеток, мы совершаем довольно прямолинейную имитацию непрерывной детерминированности с помощью дискретной, но, вообще говоря, сопоставление этих двух моделей далеко не тривиально.

Молекулярная биология доставляет образцы поведения естественных (не сконструированных человеком) систем, которое мы вынуждены описывать в терминах, близких к принятым в теории дискретных автоматов. На рис. 2 изображена схема синтеза белка на информационной РНК: она очень похожа на изображение машины Тьюринга, копирующей информацию с одной ленты на другую.

Классические непрерывные системы, управляемые дифференциальными уравнениями, могут имитировать дискретные автоматы лишь при исключительно сложной структуре своего фазового пространства: обилии областей устойчивости, разделенных невысокими энергетическими барьерами. Ввод программы проделывает изощрен-

ную систему проходов в этих барьерах, предопределяя движение фазовой траектории по этому лабиринту. Как физическая система вычислитель должен быть очень неустойчив, ибо ошибка в один знак в программе, вообще говоря, приводит к совершенно другой траектории. Но сам процесс вычисления должен быть беспримерно стабильным, т. е. самопроизвольные ошибки (переход траектории через барьер, который должен быть закрыт, в результате флюктуации) должны иметь весьма малую вероятность. Хорошо известно, что эти требования (в сочетании с медленностью работы и экспоненциальным ростом диссипируемой энергии при увеличении сложности) поста-

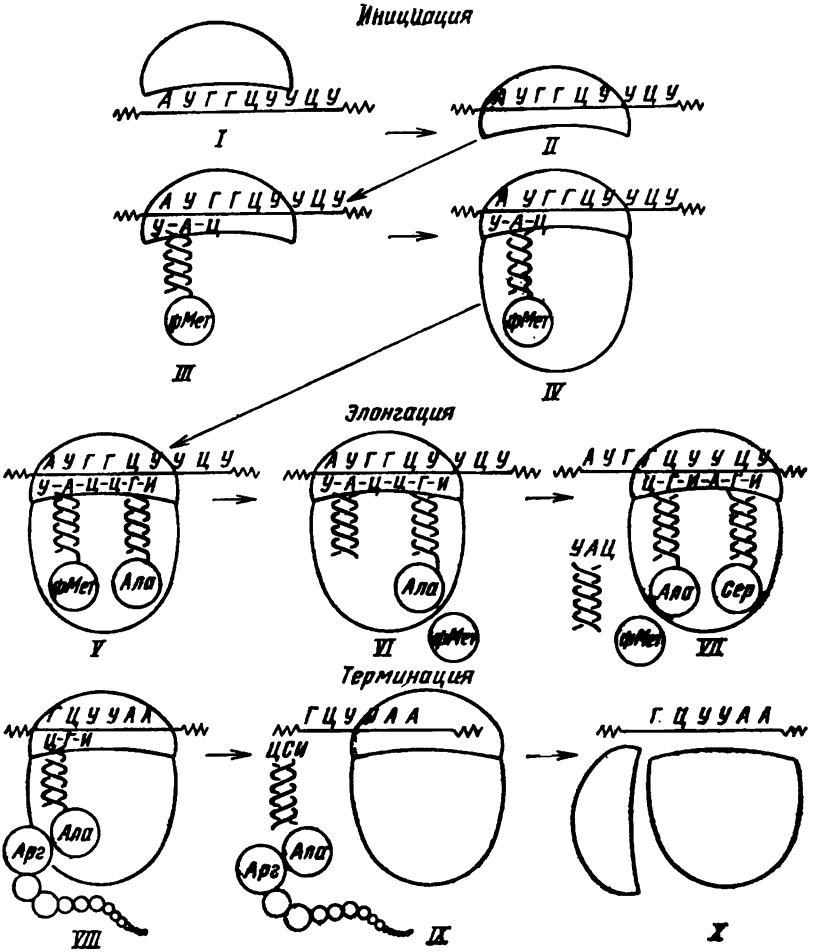

Рис. 2

вили барьер перед развитием механических компьютеров. Между тем действие «генетических автоматов» мы пытаемся часто описывать именно такими механическими терминами. К самым известным парадоксам, к которым приводит такое описание, относится гипотетическая картина разворачивания двойной спирали в процессе репликации. В этой картине двойная спираль бактериальной хромосомы закручена примерно на 300 000 оборотов. Так как ее удвоение в благоприятных обстоятельствах занимает 20 мин, согласно механической модели репликации, при разворачивании спирали часть хромосомы должна вращаться со скоростью, не меньшей 125 оборотов в секунду. Параллельно должна происходить сложная сеть безошибочных биохимических превращений.

Возможно, для прогресса в понимании таких явлений нам недостает математической теории квантовых автоматов Такие объекты могли бы показать нам математические модели детерминированных процессов с совершенно непривычными свойствами. Одна из причин этого в том, что квантовое пространство состояний обладает гораздо большей емкостью, чем классическое: там, где в классике имеется N дискретных состояний, в квантовой теории, допускающей их суперпозицию, имеется c^N планковских ячеек. При объединении классических систем их числа состояний N_1 и N_2 перемножаются, а в квантовом варианте получается $c^{N_1 N_2}$.

Эти грубые подсчеты показывают гораздо большую потенциальную сложность квантового поведения системы по сравнению с его классической имитацией. В частности, из-за отсутствия однозначного разделения системы на элементы состояние квантового автомата может рассматриваться многими способами как состояние совершенно разных виртуальных классических автоматов. (Ср. со следующим поучительным подсчетом в конце работы [17]. «Для квантовомеханического расчета молекулы метана требуется провести вычисления по методу сеток в 10^{42} точках. Если считать, что в каждой точке следует выполнить всего 10 элементарных операций, и предположить, что все вычисления производятся при сверхнизкой температуре ($T = 3 \cdot 10^{-3}$ K), то и при этом расчет молекулы метана потребует израсходовать энергию, производимую на Земле примерно за столетие».)

Первая трудность при проведении этой программы состоит в выборе правильного баланса между математическими и физическими принципами. Квантовый автомат должен быть абстрактным: его математическая модель должна использовать лишь самые общие квантовые принципы, не предрешая физических реализаций. Тогда модель эволюции есть унитарное вращение в конечномерном гильбертовом пространстве, а модель виртуального разделения на подсистемы отвечает разложению пространства в тензорное произведение. Где-то в этой картине должно найти место взаимодействие, описываемое по традиции эрмитовыми операторами и вероятностями.

Глава I

РЕКУРСИВНЫЕ ФУНКЦИИ И АЛГОРИТМЫ

1. ИНТУИТИВНАЯ ВЫЧИСЛИМОСТЬ

1.1. Основным объектом этой главы будут строгие математические понятия, которые формализуют представление о том, что некоторые функции поддаются «механическому» вычислению, скажем, на ЭВМ, как только для этого составлена надлежащая программа, тогда как другие функции, заданные неэффективным определением, могут требовать творческого подхода к задаче определения каждого своего значения.

Несколько характерных черт идеализации следует объяснить сразу.

а) Областями определения и значений рассматриваемых нами функций будут в основном целые положительные числа или составленные из них векторы фиксированной длины, или, наконец, подмножества таких векторов. Это связано, например, с представлением о том, что цифровые ЭВМ имеют дело с приближенной записью чисел, скажем, в двоичной системе, и притом с заранее ограниченной точностью. Измеряя все эти числа в единицах последнего разряда, можно считать их целыми.

б) Нас почти не будет интересовать пока вопрос о структуре самих программ и разворачивающегося во времени и пространстве процесса их работы, в частности, проблема объема памяти и длины вычислений. Лишь существование или несуществование программы, вычисляющей некоторую описанную функцию, будет главным предметом рассмотрения.

С более широкой точки зрения основные абстракции теории вычислимости будут описаны в последнем параграфе этой главы. Там мы коснемся идеализации «конструктивного объекта», которая служит адекватной моделью для представления об алгоритмах, перерабатывающих символьную информацию, а также соответствующих идеализаций и самого понятия алгоритма.

В этом параграфе мы обсудим понятие вычислимости неформально. Его главная цель — подчеркнуть важность абстрации «полувычислимости» и дать первую, самую слабую формулировку знаменитого «тезиса Черча».

1.2. Введем несколько простых основных понятий. Пусть X, Y — два множества. *Частичной функцией* (или отображением) из X в Y будем называть любую пару $\langle D(f), f\rangle$, состоящую из подмножества $D(f) \subseteq X$ и отображения $f: D(f) \to Y$. Здесь $D(f)$ называется *областью определения* f; f определена в точке $x \in X$, если $x \in D(f)$; f нигде не определена, если $D(f)$ пусто; существует единственная нигде не определенная частичная функция.

Через $Z^+ = \{1, 2, 3...\}$ будем обозначать множество натуральных чисел, *исключая нуль*. (Последнее не обязательно, но допущение нуля требует другой редакции доказательств.) Если $n \geqslant 1$, через $(Z^+)^n$ мы обозначим n-кратное прямое произведение Z^+ на себя, т. е. множество упорядоченных n-ок $\langle x_1, \ldots, x_n\rangle$, $x_i \in Z^+$. Удобно считать, что $(Z^+)^0$ — множество, состоящее из одного элемента. Нашим основным объектом будут частичные функции из $(Z^+)^m$ в $(Z^+)^n$ для различных m, n. В следующей далее классификации этих функций по степени их вычислимости под словом «программа» читатель может представлять себе программу для универсальной вычислительной машины, написанную без учета ограничений на время и память. Подразумевается, что каждая программа для вычисления функции содержит специальное «пустое место» для вставки очередного значения аргумента.

1.3. **Основное определение.** а) Частичная функция f из $(Z^+)^m$ в $(Z^+)^n$ называется *вычислимой*, если существует такая «программа», что при подаче на ее вход вектора $x \in (Z^+)^m$ мы получим на выходе $f(x)$, если $x \in D(f)$; 0, если $x \notin D(f)$.
(Здесь 0 — просто указатель того, что f не определена в x; можно было бы разрешить в этом случае получить на выходе что угодно *не из* $(Z^+)^n$.)

б) Частичная функция f из $(Z^+)^m$ в $(Z^+)^n$ называется *полувычислимой*, если существует такая «программа», что при подаче на ее вход $x \in (Z^+)^m$ мы получаем на выходе $f(x)$, если $x \in D(f)$; получаем на выходе 0 или же программа работает бесконечно долго, если $x \notin D(f)$.

В частности, *вычислимые функции полувычислимы, а всюду определенные полувычислимые функции вычислимы.*

в) Частичная функция f называется *невычислимой*, если она не удовлетворяет условию б) и тем более а).

1.4. **Пояснения.** а) Из этих трех понятий основным является полувычислимость, ибо вычислимость сводится к нему. Действительно, для выделения вычислимых функций из полувычислимых можно поступить так.

Пусть $X \subseteq Y$ — два множества. Назовем характеристической функцией подмножества X в Y такую функцию $\chi_X: Y \to Z^+$, что

$$\chi_X(x) = \begin{cases} 1, & \text{если } x \in X; \\ 2, & \text{если } x \notin X. \end{cases}$$

Заметим, что χ_X определена всюду.

Теперь пусть f — полувычислимая функция из $(Z^+)^m$ в $(Z^+)^n$. Если она даже вычислима, то вычислима и характеристическая функция ее области определения $D(f)$: к вычисляющей f программе нужно добавить инструкции «переработать 0 в 2, а не 0 в 1 и подать на выход». Наоборот, если вычислима $\chi_{D(f)}$, то вычислима и f: перед программой, полувычисляющей f, нужно написать программу, вычисляющую $\chi_{D(f)}$, и подавать на выход сразу 0, если $\chi_{D(f)}(x) = 2$, или передавать x в программу для f, если $\chi_{D(f)}(x) = 1$. Таким образом,

$$f \text{ вычислима} \Longleftrightarrow \begin{cases} f \text{ полувычислима и } \chi_{D(f)}, \\ \text{полувычислима (и, значит, } \chi_{D(f)} \text{ автоматически вычислима, ибо всюду определена).} \end{cases}$$

Правую часть этой импликации мы выберем в качестве формализации понятия вычислимости, когда полувычислимость будет формализована.

б) *Существуют невычислимые функции.* Действительно, каждая программа — это конечный текст в конечном алфавите, так что множество программ счетно, тогда как множество всех функций $Z^+ \to Z^+$ несчетно. (Критику этого рассуждения см. ниже в п. 1.5.)

Конкретный пример невычислимой функции.

Рассмотрим формальный язык арифметики $S\mathrm{Ar}$, описанный в § 10 гл. II книги Д и НД. Пронумеруем формулы этого языка, как это было объяснено в § 11 гл. II той же книги. Определим функцию f соглашением

$$f(k) = \begin{cases} 1, \text{ если } k\text{-я формула истинна в стандартной интерпретации;} \\ \text{не определена, если } k\text{-я формула ложна.} \end{cases}$$

Функция f невычислима. В гл. V мы увидим, что это следует из невыразимости множества $D(f)$, установленной теоремой Тарского.

Иначе говоря, нельзя распознать (хотя бы в принципе) все теоретико-числовые теоремы, написав одну (хотя бы очень большую и сложную) программу для их распознавания по данной формулировке.

Доказательство этого результата, конечно, требует гораздо более глубокого анализа понятия вычислимости.

в) *Существуют полувычислимые, но не вычислимые функции.* Сначала приведем пример полувычисляющей программы. Рассмотрим функцию f из Z^+ в Z^+, определенную через задачу Ферма:

$$f(n) = \begin{cases} 1, \text{ если существуют } x, y, z \in Z^+ \\ \quad \text{с условием } x^{n+2} + y^{n+2} = z^{n+2}; \\ \text{не определена иначе.} \end{cases}$$

Вот программа, полувычисляющая f: после того как на вход подано n, перебирать векторы $< x, y, z >$ в лексикографическом порядке и проверять для каждого вектора условие $x^{n+2} + y^{n+2} = z^{n+2}$. Если оно выполнено, подать на выход. 1. Иначе, переходить к следующему.

Значит, f полувычислима. Но мы до сих пор не знаем, вычислима ли f. Гипотеза Ферма состоит в том, что f нигде не определена (и, значит, вычислима!). Самые сильные теоретические результаты, известные относительно f, — так называемые критерии Куммера, Вифериха, Вандивера и др. — можно рассматривать как некоторое приближение именно к доказательству *вычислимости* f, а не того, что она нигде не определена. Поэтому для следующей проверки гипотезы Ферма для тех или иных значений n нужен еще (машинный) счет (объем которого быстро растет с ростом n) для вычисления $\chi_{D(f)}$ в точке n, когда оно возможно.

Аналогичную природу имеет пример полувычислимой функции, которая уже заведомо не является вычислимой: мы докажем в гл. II, что существует такой многочлен

$$P(t, x_1, \ldots, x_n)$$

с целыми коэффициентами, что функция

$$g(t) = \begin{cases} 1, \text{ если уравнение } P(t, x_1, \ldots, x_n) = 0 \text{ разрешимо} \\ \qquad x_1, \ldots, x_n \in Z^+; \\ \text{не определена иначе} \end{cases}$$

— не вычислима. Ее невычислимость устанавливается точно так же, как для функции f, связанной с уравнением Ферма.

1.5. Критика предшествующих доказательств:

Прежде чем двигаться дальше, рассмотрим более критически, скажем, рассуждение из п. 1.4 б). Первое слабое место бросается в глаза: мы не уточнили, что такое программа. Однако это не так существенно; при любом выбранном уточнении программа должна быть текстом над конечным алфавитом, чтобы удовлетворять интуитивным представлениям, а таких текстов счетное множество. Гораздо более сильное возражение состоит примерно в следующем: на каком основании мы можем работать с *одним* уточнением понятия программы? Возможно, существует все возрастающая иерархия точно описываемых «вычислительных средств», так что для каждой функции из Z^+ в Z^+ можно подобрать свою программу, которая может вычислять эту функцию?

Фундаментальным открытием теории вычислимости было то обстоятельство, что на последний вопрос нужно дать отрицательный ответ. К настоящему времени мы обладаем единственным и окончательным формальным понятием, которое выдержало все проверки на

его соответствие интуитивному представлению о полувычислимости и которое конструируется так.

1.6. Тезис Черча (слабейшая форма). *Можно явно указать*

а) *семейство простейших полувычислимых функций;*

б) *семейство элементарных операций, которые позволяют строить по одним полувычислимым функциям другие полувычислимые функции;*

с тем свойством, что любая полувычислимая функция получается за конечное число шагов, каждый из которых состоит в применении одной из элементарных операций к ранее построенным либо к простейшим функциям.

1.7. Пояснение. В следующем параграфе тезису Черча будет придана точная формулировка: простейшие функции и элементарные операции будут заданы явно. С одного места начнется точная математическая теория вычислимости. Однако нам казалось важным отметить принципиальное значение того открытия, что семейства таких функций и операций вообще существуют и могут быть явно указаны, что далеко не очевидно.

Это — экспериментальный факт, один из важнейших открытых логикой. Свидетельства в его пользу и его значение будут обсуждены в следующем параграфе. Сейчас отметим лишь, что он родствен финитности основных логико-множественных принципов математики (заложенных, скажем, в языке L_1 Set: см. Д и НД), но не тождествен.

2. ЧАСТИЧНО РЕКУРСИВНЫЕ ФУНКЦИИ

2.1. В этом параграфе мы изложим точное определение и первоначальные свойства класса частичных функций из $(Z^+)^m$ в $(Z^+)^n$, который считается адекватной формализацией класса полувычислимых функций. Он будет описан тем способом, который указан в формулировке тезиса Черча в п. 1.6.

2.2. Простейшие функции.

$\mathrm{suc}\colon Z^+ \to Z^+$, $\mathrm{suc}\,(x) = x + 1$;
$1^{(n)} : (Z^+)^n \to Z^+$; $1^{(n)}(x_1, \ldots, x_n) = 1$, $n \geqslant 0$;
$\mathrm{pr}_i^n : (Z^+)^n \to Z^+$, $\mathrm{pr}_i^n(x_1, \ldots, x_n) = x_i$, $n \geqslant 1$.

2.3. Элементарные операции над частичными функциями.

а) *Композиция* (или подстановка). Она ставит в соответствие паре функций f из $(Z^+)^m$ в $(Z^+)^n$ и g из $(Z^+)^n$ в $(Z^+)^p$ функцию $h = g \circ f$ из $(Z^+)^m$ в $(Z^+)^p$, которая определяется так:

$$D(g \circ f) = f^{-1}(D(g)) = \{x \in (Z^+)^m \mid$$
$$x \in D(f),\ f(x) \in D(g)\}\ (g \circ f)(x) = g(f(x)).$$

б) *Соединение.* Эта операция ставит в соответствие частичным функциям f_i из $(Z^+)^m$ в $(Z^+)^{n_i}$, $i = 1, \ldots, k$, функцию $(f_1, \ldots, f_k)$ из $(Z^+)^m$ в $(Z^+)^{n_1} \times \ldots \times (Z^+)^{n_k}$, которая определяется так:

$D((f_1, \ldots, f_k)) = D(f_1) \cap \ldots \cap D(f_k)$,
$(f_1, \ldots, f_k)(x_1, \ldots, x_m) = \langle f_1(x_1, \ldots, x_m), \ldots, f_k(x_1, \ldots, x_m) \rangle$.

в) *Рекурсия.* Эта операция ставит в соответствие паре функций f из $(Z^+)^n$, в Z^+ и g из $(Z^+)^{n+2}$ в Z^+ функцию h из $(Z^+)^{n+1}$ в Z^+, которая определяется рекурсией по последнему аргументу:

$$\begin{cases} h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n) \text{ (начальное условие);} \\ h(x_1, \ldots, x_n, k+1) = g(x_1, \ldots, x_n, k, h(x_1, \ldots, x_n, k)) \text{ при } k \geqslant 1 \\ \text{(рекурсивный шаг).} \end{cases}$$

Область определения $D(h)$ описывается также рекурсивно:

$\langle x_1, \ldots, x_n, 1 \rangle \in D(h) \Leftrightarrow \langle x_1, \ldots, x_n \rangle \in D(f)$;
$\langle x_1, \ldots, x_n, k+1 \rangle \in D(h) \Leftrightarrow \langle x_1, \ldots, x_n \rangle \in D(h)$

и $\langle x_1, \ldots, x_n, k, h(x_1, \ldots, x_n, k) \rangle \in D(g)$ при $k \geqslant 1$.

г) *Операция* μ. Эта операция ставит в соответствие частичной функции f из $(Z^+)^{n+1}$ в Z^+ частичную функцию h из $(Z^+)^n$ в Z^+, которая определяется так:

$D(h) = \{\langle x_1, \ldots, x_n \rangle \mid \exists\, x_{n+1} \geqslant 1,$
$f(x_1, \ldots, x_n, x_{n+1}) = 1$
и $\langle x_1, \ldots, x_n, k \rangle \in D(f)$ для всех $k \leqslant x_{n+1}\}$,
$h(x_1, \ldots, x_n) = \min\{x_{n+1} \mid f(x_1, \ldots, x_n, x_{n+1}) = 1\}$.

В общих чертах роль μ состоит во введении функций, заданных «неявно». Кроме того, она позволяет вводить в вычисление перебор объектов для отыскания нужного в бесконечном семействе. Три особенности операции μ заслуживают быть отмеченными немедленно.

Выбор минимального y с $f(x_1, \ldots, x_n, y) = 1$ делается, конечно, для обеспечения однозначности функции h.

Область определения h на первый взгляд представляется искусственно суженной: если, скажем, $f(x_1, \ldots, x_n, 2) = 1$, а $f(x_1, \ldots, x_n, 1)$ не определено, мы считаем $h(x_1, \ldots, x_n)$ не определенной, а не равной 2. Причина этого состоит в желании сохранить интуитивную полувычислимость функции h и будет несколько подробнее прокомментирована ниже (см. п. 2.7а).

Наконец, все описанные до μ операции, если их применять к всюду определенным функциям, дают в результате всюду определенную функцию. Для μ это, очевидно, не так: это единственная операция, ответственная за возникновение частичных функций.

2.4. Определение. а) *Последовательность частичных функций* $f_1, \ldots, f_N$ *называется частично рекурсивным (соответственно примитивно рекурсивным) описанием функции* $f_N = f$, *если* f_1 *— одна из простейших функций*;

f_i — *для всех* $i \geqslant 2$ *либо является простейшей функцией, либо получается применением одной из элементарных операций к некоторым из функций* $f_1, \ldots, f_{i-1}$ (соответственно одной из элементарных операций, кроме μ).

б) *Функция* f называется частично рекурсивной (соответственно примитивно рекурсивной), если она допускает частично рекурсивное (соответственно примитивно рекурсивное) описание.

(Аналогия с определением вывода в формальном языке бросается в глаза и может быть использована.)

2.5. Тезис Черча (обычная форма).

а) *Функция* f *полувычислима, если и только если она частично рекурсивна.*

б) *Функция* f *вычислима, если и только если* f *и* $\chi_{D(f)}$ *частично рекурсивны.*

Терминологическое замечание. Всюду определенные частично рекурсивные функции называют также *общерекурсивными*. В случае, когда область определения ясна или несущественна, употребляется просто термин «рекурсивная». Сложившееся русское словоупотребление неудачно: следовало бы говорить рекурсивная частичная функция и т. п.

2.6. Использование тезиса Черча. Прежде чем обсуждать подробнее аргументы в пользу тезиса Черча, укажем, как он используется в математической практике.

Два основных способа бросаются в глаза при изучении литературы.

а) *Тезис Черча как определение алгоритмической неразрешимости.*

Пусть имеется счетная последовательность математических «задач» $P_1, P_2, \ldots$ Предлагается далее, что каждая задача имеет ответ «да» или «нет» и что по номеру n условие задачи P_n выписывается «эффективно». Такая последовательность $P = (P_n)$ называется «массовой проблемой». Свяжем с ней функцию f из Z^+ в Z^+:

$D(f) = \{i \in Z^+ \mid P_i$ имеет ответ «да»$\}$;

$f(i) = 1$, если $i \in D(f)$.

Массовая проблема P называется *алгоритмически разрешимой*, если функция f и $\chi_{D(f)}$ частично рекурсивны. В противном случае P называется *алгоритмически неразрешимой*. Можно еще различать случаи, когда только $\chi_{D(f)}$ не является частично рекурсивной или когда даже f не частично рекурсивна. Вторая неразрешимость еще «хуже» первой; примеры были указаны в § 1. Наконец, можно строго определить и исследовать разные иерархии «степеней разрешимости».

Один известный пример массовой проблемы *проблема тождества слов в группах*. Пусть G — некоторая конечно определенная группа, $a_1, \ldots, a_r \in G$ — некоторые элементы. «Приведенное слово» от $a_1, \ldots, a_r$ — это выражение вида $a_{i_1}^{\varepsilon_1} \ldots a_{i_k}^{\varepsilon_k}$, где $k \geqslant 1$, $\varepsilon_j = \pm 1$, и если $i_j = i_{j+1}$, то $\varepsilon_j = \varepsilon_{j+1}$.

Расположим все приведенные слова в алфавитном порядке и поставим задачу P_n:

«Верно ли, что n-е слово представляет единичный элемент группы G?»

«Массовая проблема» (P_n) алгоритмически разрешима для одних групп G и элементов $a_1, \ldots, a_n$ и не разрешима для других (Новиков, Хигмэн). Функция f здесь всегда частично рекурсивна, но $\chi_{D(f)}$ — не обязательно, см. гл. VI.

Другой пример неразрешимой проблемы, связанный с диофантовыми уравнениями, описан в следующей главе.

б) *Тезис Черча как эвристический принцип.* Интуитивно понятие «полувычислимости» представляется более широким, чем понятие «частичной рекурсивности», и многие задачи о частично рекурсивных функциях становятся значительно легче, если подставить в их условие неформальные представления и разрешить пользоваться ими в решении. Скажем, формула

$$e = \lim\left(1 + \frac{1}{n}\right)^n$$

и алгоритм Эвклида делают интуитивно ясным, что функции

$f, g : Z^+ \to Z^+$:

$f(n) = n$-й десятичный знак разложения e; $g(n) = n$-е простое число, вычислимы, тогда как проверка их рекурсивности требует довольно кропотливых конструкций.

Тезис Черча позволяет разбить решение таких задач на два этапа: отыскание неформального решения с использованием любых интуитивных алгоритмов; последующая формализация. Второй этап предполагает известную опытность в отыскании частично рекурсивного описания самых разнообразных полувычислимых функций, а тезис Черча дает уверенность в том, что такое описание существует.

По мере накопления доказательств рекурсивности в литературе все чаще ограничиваются проведением лишь первого этапа решения: ярким примером тому служит книга Х. Роджерса [2].

К концу книги мы также позволим себе ряд вольностей такого рода. Все в этом есть известные опасности. Можно думать, что распространение привычки к неформальным аргументам задержало открытие такого фундаментального факта, как совпадение перечислимых множеств с диофантовыми.

2.7. Аргументы в пользу тезиса Черча. а) Прежде всего представляется ясным, что простейшие функции должны быть вычислимы, как бы ни уточнять это понятие. Далее, элементарные операции, примененные к полувычислимым функциям, снова дают полувычислимую функцию: программа, полувычисляющая ее, без труда компонуется из полувычисляющих для данных функций. Мы рассмотрим подробнее только случай μ-оператора, оставив легкую конструкцию остальных трех программ читателю.

В обозначениях п. 2 3 пусть f — полувычислимая функция из $(Z^+)^{n+1}$ в Z^+. Для вычисления h $(x_1, \ldots, x_n)$ будем перебирать в порядке возрастания последней координаты векторы $< x_1, x_2, \ldots, x_n, 1 >, < x_1, \ldots, x_n, 2 >, \ldots$ и вычислять значения f в них. Если $< x_1, \ldots, x_n > \in D(h)$, где h получается из f применением μ-оператора, то программа для f последовательно вычисляет $f(x_1, \ldots, x_n, 1), \ldots, f(x_1, \ldots, x_n, y-1)$ и, наконец, $f(x_1, \ldots, x_n, y) = 1$. Наименьшее такое y, если оно существует, нужно подать на выход: это будет значение h в точке $< x_1, \ldots, x_n >$ (до достижения $f = 1$). Если h окажется неопределенным, то полувычисляющая f программа либо будет работать бесконечно долго, либо даст ответ не из Z^+ — его нужно послать на выход; но по нашему соглашению h в точке $< x_1, \ldots, x_n >$ тогда не определена, и такое поведение программы для h согласуется с определением полувычислимости h.

Из всего сказанного нужно сделать вывод, что *частично рекурсивные функции полувычислимы*. Наиболее сильное утверждение тезиса Черча состоит, таким образом, в том, что *полувычислимые функции частично рекурсивны* (определение вычислимости через полувычислимость мы просто перенесли без изменений из § 1). Как было сказано, это экспериментальный факт. Экспериментальные свидетельства в его пользу делятся на несколько классов, которые мы рассмотрим последовательно в подпунктах б) — г).

б) В литературе имеется огромный набор рекурсивных описаний различных (полу) вычислимых функций. (См., например, книгу Р. Петер [25].) Часть этого списка мы приведем в следующем параграфе. Имеется также набор приемов составления рекурсивных описаний, применимых к целым классам (полу) вычислимых функций. Каждый раз, когда какой-нибудь автор пытался найти частично рекурсивное описание (полу) вычислимой функции, это описание находилось.

в) Тьюринг предложил математическое описание абстрактной вычислительной машины и выдвинул сильные аргументы в пользу того, что эта машина является универсальной (т. е. может (полу) вычислять все (полу) вычислимые функции), детально проанализировав характерные черты процесса детерминированного вычисления. (Еще раз обратите внимание на то, что мы совершенно не занимались формализацией процессов вычисления, а только их результатами.)

Оказалось, что класс функций, полувычислимых машинами Тьюринга, в точности совпадает с классом частично рекурсивных функций.

г) Черч, Пост, Марков, Колмогоров, Успенский и др. предложили другие детерминированные схемы переработки информации (не обязательно числовой) общего характера. Во всех случаях оказалось, что при подходящей «эффективной» нумерации множеств входов и выходов эти способы приводят к такому классу отображений из Z^+ в

Z^+, который совпадает с соответствующим подклассом частично рекурсивных функций.

За дальнейшим обсуждением тезиса Черча мы отсылаем читателя к литературе; см. в особенности С. Клини [26].

3. ОБРАЗЦЫ РЕКУРСИВНОСТИ

3.1. В этом параграфе будут приведены краткий список рекурсивных функций и выборка первоначальных примеров демонстрации рекурсивности. В дальнейшем изложении оба списка будут пополняться по мере надобности: см., в частности, гл. VII.

3.2. а).

$\mathrm{sum}_2 : (Z^+)^2 \to Z^+, \langle x_1, x_2 \rangle \mapsto x_1 + x_2.$

Рекурсия по x_2, исходя из начального условия

$x_1 + 1 = \mathrm{suc}\ (x_1),$

посредством рекурсивного шага

$x_1 + k + 1 = \mathrm{suc}\ (\mathrm{sum}_2\ (x_1, k)).$

б).

$\mathrm{sum}_n : (Z^+)^n \to Z^+, \langle x_1, \ldots, x_n \rangle \mapsto \sum_{i=1}^{n} x_i, n \geqslant 3.$

Считая известным, что sum_{n-1} рекурсивна, получаем sum_n с помощью соединений и композиции

$\mathrm{sum}_n = \mathrm{sum}_2 \circ (\mathrm{sum}_{n-1} \circ (\mathrm{pr}_1^n, \ldots, \mathrm{pr}_{n-1}^n), x_n).$

Другой вариант — рекурсия по x_n, исходя из начального значения $\mathrm{suc} \circ \mathrm{sum}_{n-1}$, посредством рекурсивного шага

$$\sum_{i=1}^{n-1} x_i + k + 1 = \mathrm{suc}\,(\mathrm{sum}_n\,(x_1, \ldots, x_{n-1}, k)).$$

Эта многозначность рекурсивных описаний, даже «естественных», будет все возрастать.

3.3.

а) $\mathrm{prod}_2 : (Z^+)^2 \to Z^+, \langle x_1, x_2 \rangle \mapsto x_1 x_2.$

Рекурсия по x_2, исходя из начального условия x_1, посредством рекурсивного шага

$x_1\,(k + 1) = x_1 k + x_1 = \mathrm{sum}_2\,(x_1 k, x_1).$

б) $\mathrm{prod}_n : (Z^+)^n \to Z^+ \langle x_1, \ldots, x_n \rangle \to x_1, \ldots, x_n, n \geqslant 3$:

$\mathrm{prod}_n = \mathrm{prod}_2 \circ (\mathrm{prod}_{n-1}(\mathrm{pr}_1^n, \ldots, \mathrm{pr}_{n-1}^n), x_n).$

3.4 а) $Z^+ \to Z^+$:

$$x \mapsto x \dot{-} 1 = \begin{cases} x-1, & \text{если } x \geqslant 2; \\ 1, & \text{если } x = 1. \end{cases}$$

Рекурсия к функциям:

$f : (Z^+)^0 \to Z^+ : \cdot \mapsto 1$;

$g = \mathrm{pr}_1^2 : (Z^+)^2 \to Z^+, \ < x_1, x_2 > \mapsto x_1$.

б) $(Z^+)^2 \to Z^+$:

$$\langle x_1, x_2 \rangle \mapsto x_1 \dot{-} x_2 = \begin{cases} x_1 - x_2, & \text{если } x_1 > x_2; \\ 1, & \text{если } x_1 \leqslant x_2. \end{cases}$$

Эта «усеченная разность» получается применением рекурсии к функциям

$f(x_1) = x_1 \dot{-} 1$,

$g(x_1, x_2, x_3) = x_3 \dot{-} 1$.

3.5. $F : (Z^+)^n \to Z^+$, *где* F *— любой многочлен от* $x_1, \ldots, x_n$ *с целыми коэффициентами, принимающий только значения из* Z^+.

Если все коэффициенты F неотрицательны, то F есть сумма произведений функций $\mathrm{pr}_i^n : < x_1, \ldots, x_n > \mapsto x_i$.

Иначе $F = F^+ - F^-$, где коэффициенты у F^+ и F^- неотрицательны, а значение неусеченной разности во всех точках $(Z^+)^n$ совпадает со значением усеченной разности $F^+ \dot{-} F^-$ по предположению об F.

Мы часто будем пользоваться рекурсивностью функций $(x_1 - x_2)^2 + 1$ или $h = (f - g)^2 + 1$, где f, g рекурсивны: этот прием позволяет отождествить «множество совпадения» $f = g$ с «множеством 1-уровня» $h = 1$, с которым удобнее работать.

3.6. «*Ступенька*»:

$$s_{x_0}^{a,\,b}(x) = \begin{cases} a \text{ при } x \leqslant x_0, \\ b \text{ при } x > x_0; \ a, b, x \in Z^+. \end{cases}$$

При $x_0 = 1$ она получается рекурсией с начальным значением a и последующими b. В общем случае

$$s_{x_0}^{a,\,b}(x) = s_1^{a,\,b}(x + 1 \dot{-} x_0).$$

3.7. $\mathrm{rem}\,(x, y)$ = *остаток от деления* y на x, *лежащий в* $[1, x]$ (у нас нет нуля!).

Имеем

$\mathrm{rem}\,(x, 1) = 1$,

$$\mathrm{rem}\,(x, y+1) = \begin{cases} 1, & \text{если } \mathrm{rem}\,(x, y) = x; \\ \mathrm{suc} \circ \mathrm{rem}\,(x, y), & \text{если } \mathrm{rem}\,(x, y) \neq x. \end{cases}$$

Применим следующий искусственный прием. Рассмотрим ступеньку $s(x) = 2$ при $x \geqslant 2$, $s(1) = 1$ и положим

$$\varphi(x, y) = s((\mathrm{rem}(x, y) - x)^2 + 1).$$

Очевидно,

$$\mathrm{rem}(x, y) \neq x \Leftrightarrow \varphi(x, y) = 1,$$
$$\mathrm{rem}(x, y) = x \Leftrightarrow \varphi(x, y) = 2,$$

откуда

$$\mathrm{rem}(x, y+1) = 2\,\mathrm{suc}(\mathrm{rem}(x, y) \dot{-} \varphi(x, y)\,\mathrm{suc}(\mathrm{rem}(x, y))).$$

Это дает определение rem рекурсией.

Опишем этот прием в более общем виде.

3.8. Пусть h задана «рекурсией с альтернативами»:

$$h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n);$$
$$h(x_1, \ldots, x_n, k+1) = g_i(x_1, \ldots, x_n, k, h(x_1, \ldots, x_n, k)),$$

если выполнено условие $C_i(x_1, \ldots, x_n, k; h)$, $i = 1, \ldots, m$. Взаимоисключающие условия C_i приведем к виду C_i выполнено $\Leftrightarrow \varphi_i(x_i, \ldots, x_n; k; h(x_1, \ldots, x_n, k)) = 1$, φ_i — всюду определенная рекурсивная функция, принимающая только значения 1 и 2. Тогда рекурсивный шаг можно записать так:

$$h(x_1, \ldots, x_n, k+1) = 2 \sum_{i=1}^{m} g_i(x_1, \ldots, x_n, k, h(x_1, \ldots, x_n, k)) \dot{-}$$
$$\dot{-} \sum_{i=1}^{m} (g_i \varphi_i)(x_1, \ldots, x_n, k, h(x_1, \ldots, x_n, k)).$$

Этот прием позволяет установить примитивную рекурсивность следующих функций, которые понадобятся нам дальше.

3.9. Неполное частное:

$$qt(x, y) = \begin{cases} \text{целая часть } y/x, & \text{если } y/x \geqslant 1, \\ 1, & \text{если } y/x < 1. \end{cases}$$

Имеем

$$qt(x, 1) = 1;$$

$$qt(x, y+1) = \begin{cases} qt(x, y), & \text{если } \mathrm{rem}(x, y+1) \neq x; \\ qt(x, y) + 1, & \text{если } \mathrm{rem}(x, y+1) \neq x,\ y+1 \neq x; \\ 1, & \text{если } y+1 = x. \end{cases}$$

К стандартному виду 3.8 условия приводятся с помощью функций

$$\tilde{s}((\mathrm{rem}(x, y+1) - x)^2 + 1),$$
$$s((\mathrm{rem}(x, y+1) - x)^2 + 1),\ \tilde{s}((x - y - 1)^2 + 1),$$
$$s((x - y - 1)^2 + 1),$$

где

$s(1)=1 \quad s(\geqslant 2)=2$: $\tilde{s}(1)=2, \ \tilde{s}(\geqslant 2)=1$.

3.10. $\operatorname{rad} x =$ *целая часть* $\sqrt{x}$.

Имеем

$$\operatorname{rad}(1)=1,$$

$$\operatorname{rad}(x+1)=\begin{cases} \operatorname{rad} x, \text{ если } qt(\operatorname{rad} x+1,\ x+1)<\operatorname{rad} x+1; \\ \operatorname{rad} x+1, \text{ если } qt(\operatorname{rad} x+1,\ x+1)=\operatorname{rad} x+1. \end{cases}$$

Предоставляем читателю привести условия к стандартному виду.

3.11. а) $\min(x, y)$:

$$\min(x, 1) = 1;$$

$$\min(x, y+1)=\begin{cases} \min(x, y), & \text{если } x\leqslant y; \\ \min(x, y)+1, & \text{если } x>y. \end{cases}$$

б) $\max(x, y)$ аналогично.

3.12. *Если* $f(x_1, \ldots, x_n)$ *рекурсивна, то*

$$Sf=\sum_{k=1}^{x_n} f(x_1, \ldots, x_{n-1}, k), \quad Pf=\prod_{k=1}^{x_n} f(x_1, \ldots, x_{n-1}, k) \text{ рекурсивны.}$$

Действительно,

$$Sf(x_1, \ldots, x_{n-1}, x_n+1) = Sf(x_1, \ldots, x_n) + f(x_1, \ldots, x_n+1),$$

$$Pf(x_1, \ldots, x_{n-1}, x_n+1) = Pf(x_1, \ldots, x_n) \cdot f(x_1, \ldots, x_n+1).$$

3.13. *Если* $f(x_1, \ldots, x_n)$ *рекурсивна, то рекурсивны функции, которые получаются из* f:

а) *любой перестановкой аргументов*;

б) *введением любого числа фиктивных аргументов*;

в) *отождествлением членов любой группы аргументов* ($f(x, x)$ *вместо* $f(x, y)$ *и т. п.*).

Действительно, все эти функции можно получить из f и различных pr_i^m композицией и соединением.

3.14. *Отображение* $f: (Z^+)^m \to (Z^+)^n$ *рекурсивно, если и только если все его компоненты* $\operatorname{pr}_i^n \circ f$ *рекурсивны.* (Очевидно.)

Отметим в заключение, что все конкретные функции, описанные до сих пор, были примитивно рекурсивными и все описанные операции, если применяются к примитивно рекурсивным функциям, дают также примитивно рекурсивный результат. Начиная со следующего параграфа, мы будем существенно пользоваться операцией μ.

4. ПЕРЕЧИСЛИМЫЕ И РАЗРЕШИМЫЕ МНОЖЕСТВА

4.1. Определение. *Множество* $E \subseteq (Z^+)^n$ *называется перечислимым, если существует такая частично рекурсивная функция* f, что $E = D(f)$ (*область определения* f).

Обсуждение в § 1 и 2 показывает, что интуитивный смысл перечислимости E таков: существует программа, которая распознает элементы x, принадлежащие E, но, возможно, не умеет распознавать элементы, не принадлежащие E. Позже, в п. 4.12 и 4.18, будет дано другое интуитивное описание перечислимых множеств, более ясно указывающее на этимологию названия: это *множества, все элементы которых могут быть получены (возможно, с повторениями и в неизвестном порядке) с помощью некоторой «порождающей» их программы.*

Понятие перечислимого множества наряду с понятием частично рекурсивной функции занимает центральное место во всей теории Из дальнейших результатов, в частности предложения 4.15, будет видно, что любое из них может быть приведено к другому, однако в доказательствах необходимую гибкость дает лишь использование обоих понятий.

Начнем со следующего простого факта.

4.2. Предложение. *Следующие три класса множеств совпадак....*

а) *Перечислимые множества.*

б) *Множества уровня частично рекурсивных функций.*

в) *Множества 1-уровня частично рекурсивных функций.*

Доказательство. Напомним, что множеством m-уровня (или просто m-уровнем) функции f из $(Z^+)^n$ в Z^+ называется множество $E \subseteq D(f)$, такое, что

$$x \in E \Leftrightarrow f(x) = m.$$

а) $\subset$ в). Пусть E перечислимо, $E = D(f)$, где f частично рекурсивна. Тогда

E = 1-уровень функции $1^{(1)} \cdot f$.

б) = в). m-уровень f совпадает с 1-уровнем $(f - m)^2 + 1$. Функция $(f - m)^2 + 1$ частично рекурсивна в силу предложения 3.5 вместе с f.

в) $\subset$ а). Пусть E — 1-уровень частично рекурсивной функции $f(x_1, \ldots, x_n)$. Положим

$$g(x_1, \ldots, x_n) = \min \{y \mid (f(x_1, \ldots, x_n) - 1)^2 + y = 1\}.$$

Очевидно, g частично рекурсивна и $E = D(g)$.

Основным результатом этого параграфа будет следующее гораздо более трудное утверждение и его следствия.

4.3. Теорема. *Следующие два класса множеств совпадают:*

а) *Перечислимые множества.*

б) *Проекции множеств уровня примитивно рекурсивных функций со значениями в* Z^+.

4.4. Первая часть доказательства. Напомним прежде всего, что если дано некоторое множество
$E \subset (Z^+)^{n+m}$,
то его проекцией («на пространство первых n координат») называется множество $F \subset (Z^+)^n$, которое определяется так:

$$\langle x_1, \ldots, x_n \rangle \in F \Longleftrightarrow \exists\, \langle y_1, \ldots, y_m \rangle \in (Z^+)^m,\ \langle x_1, \ldots, y_m \rangle \in E.$$

(Здесь и ниже мы, в расхождение с практикой первой части, не отмечаем в обозначениях разницы между «переменными координат» и их частными значениями.) Аналогично определяется проекция «на координаты с номерами $(i_1, \ldots, i_n) \subset (1, \ldots, n)$». Число m удобно называть *коразмерностью* проекции. Каноническое отображение $E \to F$ также принято называть проекцией: это не может привести к путанице.

Назовем временно проекции уровней примитивно рекурсивных функций *примитивно перечислимыми* множествами.

Первая часть доказательства будет состоять в установлении того факта, что примитивно перечислимые множества перечислимы; вторая — в проверке обратного включения.

Итак, пусть $f(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m})$ — некоторая примитивно рекурсивная функция, E — проекция ее 1-уровня на первые n координат. (1-уровнями можно ограничиться в силу уже использованного соображения: k-уровень f совпадает 1-уровнем $f' = (f - k)^2 + 1$). Построим явно такую частично рекурсивную функцию g, что $E = D(g)$.

Разберем отдельно три случая, в зависимости от коразмерности проекции: $m = 0$, 1 или $m \geqslant 2$.

Случай а): $m = 0$. Тогда $E = 1$-уровень $f \Longleftrightarrow E$ перечислимо по предложению 4.2 (g построена там явно).

Случай б): $m = 1$. Положим

$$g(x_1, \ldots, x_n) = \min \{x_{n+1} \mid f(x_1, \ldots, x_n, x_{n+1}) = 1\}.$$

Очевидно, g частично рекурсивна и $D(g) = E$ (обратите внимание на то, как здесь используется обстоятельство $D(f) = (Z^+)^{n+1}$).

Случай в): $m \geqslant 2$. Мы сведем этот случай к предыдущему с помощью следующей леммы, важной во многих других вопросах и имеющей принципиальный интерес (отсутствие понятия размерности в «рекурсивной геометрии»).

4.5. Лемма. *Для всех $m \geqslant 1$ существует такое взаимно однозначное отображение $t^{(m)} : Z^+ \to (Z^+)^{(m)}$, что:*

а) *Функции $t_i^{(m)} = \mathrm{pr}_i^{(m)} \circ t^{(m)}$ примитивно рекурсивны для всех $1 \leqslant i \leqslant m$.*

б) *Обратная функция $\tau^{(m)} : (Z^+)^n \to Z^+$ примитивно рекурсивна.*

4.6. Использование леммы. Предположим, что лемма верна. Применим ее к ситуации п. 4.4в). Так, положим (при $m \geqslant 2$)

$$g(x_1, \ldots, x_n, y) = f(x_1, \ldots, x_n, t_1^{(m)}(y), \ldots, t_m^{(m)}(y)).$$

Очевидно, g примитивно рекурсивна вместе с f. Легко проверяется, что E совпадает с проекцией 1-уровня функции g на первые n координат. Так как это проекция коразмерности 1, мы свели этот случай к уже разобранному.

4.7. Доказательство леммы. Случай $m = 1$ тривиален. Проведем индукцию по m, начиная с $m = 2$.

Конструкция $t^{(2)}$. Сначала построим явно $\tau^{(2)} : (Z^+)^2 \to \to Z^+$, положив

$$\tau^{(2)}(x_1, x_2) = 0{,}5\,((x_1 + x_2)^2 - x_1 - 3x_2 + 2).$$

Легко проверяется, что если пронумеровать пары $\langle x_1, x_2\rangle \in \in (Z^+)^2$ в «канторовском порядке», расположив их по возрастанию $x_1 + x_2$, а внутри группы с данным $x_1 + x_2$ — по возрастанию x_1, то $\tau^{(2)}(x_1, x_2)$ будет как раз номером пары $\langle x_1, x_2\rangle$ в этом списке. Тем самым, $\tau^{(2)}$ взаимно однозначна и примитивно рекурсивна (использовать предложение 3.5 и рекурсивность qt, п. 3.10 для учета 1/2).

Восстановление пары $\langle x_1, x_2\rangle$ по ее номеру y является элементарной задачей и приводит к следующим формулам для обратной функции $t^{(2)}$:

$$t_1^{(2)}(y) = y - \frac{1}{2}\left[\sqrt{2y - \frac{7}{4}} - \frac{1}{2}\right]\left(\left[\sqrt{2y - \frac{7}{4}} - \frac{1}{2}\right] + 1\right),$$

$$t_2^{(2)}(y) = \left[\sqrt{2y - \frac{7}{4}} - \frac{1}{2}\right] - t_1^{(2)}(y) + 2.$$

Здесь $[z]$ означает целую часть z. Проверку примитивной рекурсивности этих функций с помощью результатов (и приемов) § 3 мы оставляем читателю в качестве упражнения.

Конструкция $t^{(m)}$, $m \geqslant 3$. Предположим, что $t^{(m-1)}$, $\tau^{(m-1)}$ уже построены и проверены их свойства. Положим прежде всего

$$\tau^{(m)}(x_1, \ldots, x_m) = \tau^{(2)}(\tau^{(m-1)}(x_1, \ldots, x_{m-1}),\ x_m).$$

Ясно, что $\tau^{(m)}$ примитивно рекурсивна и взаимно однозначна. Решив уравнение

$$\tau^{(2)}(\tau^{(m-1)}(x_1, \ldots, x_{m-1}), x_m) = y$$

в два приема, получим для обратной функции $t^{(m)}$ формулы

$$t_m^{(m)}(y) = t_2^{(2)}(y),$$

$$t_i^{(m)}(y) = t_i^{(m-1)}(t_2^{(2)}(y)), \quad 1 \leqslant i \leqslant m-1.$$

По индуктивному предположению $t_i^{(m)}$ примитивно рекурсивны.

Этим завершается доказательство леммы и вместе с ним первая часть доказательства теоремы 4.3.

Вторая часть доказательства. Теперь мы должны установить, что всякое перечислимое множество примитивно перечислимо.

Начнем со следующего свойства класса примитивно перечислимых множеств.

4.8. Лемма. *Класс примитивно перечислимых множеств замкнут относительно следующих операций: конечное прямое произведение, конечное пересечение, конечное объединение, проекция.*

Доказательство. Пусть $E, E' \subseteq (Z^+)^n$, $E_1 \subset (Z^+)^m$ — три примитивно перечислимых множества, проекции 1-уровней примитивно рекурсивных функций f, f' и f_1 соответственно:

$$x = \langle x_1, \ldots, x_n\rangle \in E \Leftrightarrow \exists y = \langle y_1, \ldots, y_r\rangle,\ f(x, y) = 1,$$
$$x = \langle x_1, \ldots, x_n\rangle \in E \Leftrightarrow \exists z = \langle z_1, \ldots, z_q\rangle,\ f'(x, z) = 1,$$
$$u = \langle u_1, \ldots, u_m\rangle \in E_1 \Leftrightarrow \exists v = \langle v_1, \ldots, v_s\rangle,\ f_1(u, v) = 1.$$

Тогда имеем

$E \times E_1$ = проекция 1-уровня функции $(f \cdot f_1)(x, u; y, v)$:
$E \cup E'$ = проекция 1-уровня функции $(f - 1)(f' - 1) + 1$;
$E \cap E'$ = проекция 1-уровня функции $(f \circ f')(x; y, z)$.

Устойчивость относительно проекций заложена в определении.

Пусть теперь E — некоторое перечислимое множество. Реализуем его как 1-уровень частично рекурсивной функции f из $(Z^+)^n$ в Z^+ по предложению 4.2 и заметим, что для доказательства примитивной перечислимости E достаточно проверить примитивную перечислимость *графика*. $\Gamma_f \subset (Z^+)^n \times Z^+$. Действительно, ясно, что E = 1-уровень f = проекция на первые n координат множества $\Gamma_f \cap |(Z^+)^n \times \{1\}|$. Кроме того, множество $\{1\} \subset Z^+$ примитивно перечислимо, например, по п. 3.6. Если мы докажем, что Γ_f примитивно перечислимо, из леммы 4.8 будет следовать то же самое для E. Итак, окончательная редукция нашей задачи выглядит так: *доказать, что графики частично рекурсивных функций f примитивно перечислимы*. С этой целью мы проверим, что а) графики простейших функций примитивно перечислимы; б) если даны функции с примитивно перечислимыми графиками, то у функции, которая получается из них применением одной из элементарных операций, так же примитивно перечислимый график.

Графики простейших функций.

$\Gamma\,\mathrm{suc} \subset (Z^+)^2$ = 1-уровень $(x_1 + 1 - x_2)^2 + 1$;
$\Gamma\,\mathrm{suc} \subset (Z^+)^{n+1}$ = 1-уровень x_{n+1};
$\Gamma\,\mathrm{pr}_1^n \subset (Z^+)^{n+1}$ = 1-уровень $(x_i - x_{n+1})^2 + 1$.

Устойчивость относительно соединения. Пусть f, g — частичные отображения из $(Z^+)^m$ в $(Z^+)^p$ и $(Z^+)^q$ соответственно. Предположим, что Γ_f и Γ_g примитивно перечислимы. Тогда $\Gamma_{(f, g)} \subset (Z^+)^m \times (Z^+)^p \times (Z^+)^q$ совпадает с пересечением

$(\Gamma_f \times (Z^+)^q) \cap \mathrm{perm}\,(\Gamma_g \times (Z^+)^p)$.

Здесь perm : $(Z^+)^m \times (Z^+)^q \times (Z^+)^p \to (Z^+)^m \times (Z^+)^p \times (Z^+)^q$ операция, которая меняет местами два последних сомножителя:

$$\langle x^{(m)}, y^{(q)}, z^{(p)} \rangle \to \langle x^{(m)}, z^{(p)}, y^{(q)} \rangle.$$

Из леммы 4.8 видно, что $\Gamma_{(f, g)}$ примитивно перечислим.

Устойчивость относительно композиции. Пусть g — частичное отображение из $(Z^+)^n$ в $(Z^+)^m$, f — то же из $(Z^+)^m$ в $(Z^+)^p$, $h = f \cdot g$. Тогда Γ_h = проекция множества $(\Gamma_g \times (Z^+)^p) \cap ((Z^+)^n \times \Gamma_f)$ на $(Z^+)^n \times (Z^+)^p$.

Как выше, если Γ_f и Γ примитивно перечислимы, то же верно для Γ_h по лемме 4.6.

Устойчивость относительно рекурсии и μ-оператора является значительно более тонким фактом. Нам понадобится следующая красивая и полезная лемма.

4.9. Лемма. *Существует примитивно рекурсивная функция* Gd (k, t) (*функция Геделя*) со следующим свойством:

для любого $N \in Z^+$ *и любой конечной последовательности* $a_1, \ldots, a_N \in Z^+$ *длины* N *существует такое* $t \in Z^+$, что Gd $(k, t) = a_k$ *при всех* $1 \leqslant k \leqslant N$ (иными словами, Gd (k, t) — это такая последовательность функций от аргумента k, пронумерованная значениями параметра t, что любая функция от k на сколь угодно большом интервале $1, \ldots, N$ может быть имитирована подходящим членом последовательности).

Доказательство. Сначала положим

$$\text{gd}(u, k, t) = \text{rem}(1 + kt, u)$$

и покажем, что gd обладает тем же свойством, что и Gd, если разрешить подбирать $\langle u, t \rangle \in (Z^+)^2$. После этого можно будет положить

$$\text{Gd}(k, y) = \text{gd}(t^{(2)}_1(y), k, t^{(2)}_2(y)),$$

где $t^{(2)} : Z^+ \to (Z^+)^2$ — изоморфизм из леммы 4.5. Избавление от лишнего параметра u в Gd (k, t) по сравнению с gd (u, k, t) несущественно, но в дальнейшем укоротит некоторые формулы.

Итак, пусть даны $a_1, \ldots, a_N \in Z^+$. Сначала выберем $X \in Z^+$ с условиями $X \geqslant N$, $1 + kX! > a_k$ для всех $1 \leqslant k \leqslant N$. Далее положим $t = X!$. Легко видеть, что если $k_1 \neq k_2$, $k_1, k_2 \leqslant N$, то $1 + k_1X!$ и $1 + k_2X!$ взаимно просты: их общий делитель должен был бы делить $(k_1 - k_2)X!$, т. е. состоять из простых чисел $\leqslant X$, но они одно из них не делит $1 + k_1X!$.

По элементарной теореме теории чисел существует решение $u \in Z^+$ системы сравнений

$$u \equiv a_k \bmod (1 + kX!), \quad 1 \leqslant k \leqslant N.$$

Очевидно, отсюда вытекает, что

$$\text{gd}(u, k, t) = \text{rem}(1 + kt, u) = a_k, \quad 1 \leqslant k \leqslant N.$$

Теперь продолжим доказательство теоремы 4.3.

4.10. Устойчивость относительно μ-операции.

Пусть f — частичная функция из $(Z^+)^{n+1}$ в Z^+ и пусть

$$g(x_1, \ldots, x_n) = \min \{y \mid f(x_1, \ldots, x_n, y) = 1\}.$$

Напомним, что область определения g состоит из тех $\langle x_1, \ldots, x_n \rangle$, для которых такой y существует, и $\langle x_1, \ldots, x_n, k \rangle \in D(f)$ для всех k, меньших $\min y$.

Мы хотим доказать, что если Γ_f примитивно перечислим, то Γ_g так же примитивно перечислим.

Пусть Γ_f является проекцией 1-уровня (на первые $n+1$ координат) примитивно-рекурсивной функции F:

$$\varphi = f(x_1, \ldots, x_{n+1}) \Leftrightarrow \exists \langle y_1, \ldots, y_m \rangle,$$
$$F(x_1, \ldots, x_{n+1}, \varphi, y_1, \ldots, y_m) = 1$$

(буквой φ мы обозначим тот аргумент F, который становится значением f). Как и в п. 4.4, достаточно рассмотреть случай $m = 1$: если $m = 2$, то воспользоваться леммой 4.5 для замены вектора $\langle y_1, \ldots, y_m \rangle$ одним числом y, а если $m = 0$, то ввести «фиктивный аргумент» y, от которого F на самом деле не зависит.

Итак, пусть $m = 1$. Введем функцию G от аргументов $x_1, \ldots, x_n, \gamma, y, t, t_1$, положив

$$s(1) = 2, \quad s(x) = 1$$
при $x \geqslant 2$,
$$F_k = F(x_1, \ldots, x_n, k, \mathrm{Gd}(k, t), \mathrm{Gd}(k, t_1)), \quad k \geqslant 1,$$

$$G = F(x_1, \ldots, x_n, \gamma, 1, y) \prod_{k=1}^{\gamma-1} s(\mathrm{Gd}(k, t)) \cdot F_k.$$

Здесь $\prod_{k=1}^{0} = 1$ по определению.

Легко убедиться, что G примитивно рекурсивна; она получается рекурсией по аргументу γ из двух других функций, примитивная рекурсивность которых очевидна.

Мы покажем, что Γ_g является проекцией на координаты $(x_1, \ldots, x_n, \gamma)$ 1-уровня функции G.

Включение $\mathrm{pr}(G = 1) \subseteq \Gamma_g$. Пусть $\langle x_1, \ldots, x_n, \gamma, y, t, t_1 \rangle$ — фиксированная точка на 1-уровне G. Мы должны проверить, что $\langle x_1, \ldots, x_n \rangle \in D(g)$ и что $\gamma = g(x_1, \ldots, x_n)$.

Иными словами, нужно установить, что

$$f(x_1, \ldots, x_n, \gamma) = 1;$$

$f(x_1, \ldots, x_n, k)$ определена и больше 1 для всех $k \leqslant \gamma - 1$.

Так как $G = 1$ в данной точке, все сомножители $G = 1$ в этой точке. В частности, $F(x_1, \ldots, x_n, \gamma, 1, y) = 1$, откуда и следует, что $f(x_1, \ldots$

$\ldots, x_n, \gamma) = 1$, ибо Γ_f есть проекция 1-уровня F. Если $\gamma = 1$, больше проверять нечего.

Пусть $\gamma > 1$. Обращение в 1 k-го сомножителя в $\prod_{k=1}^{\gamma-1}$ дает

$s(\mathrm{Gd}(k; t)) = 1 \Rightarrow \mathrm{Gd}(k, t) \geqslant 2,$
$F_k = 1 \Rightarrow \mathrm{Gd}(k, t) = f(x_1, \ldots, x_n, k) \geqslant 2.$

Это доставляет требуемое.

Включение $\Gamma_g \subseteq \mathrm{pr}(G = 1)$. Пусть $\langle x_1, \ldots, x_n, \gamma \rangle \in \Gamma_g$. Мы должны подобрать значения остальных координат y, t, t_1 так, чтобы сделать все сомножители в соответствующей точке равными 1.

Прежде всего $\langle x_1, \ldots, x_n, \gamma, 1 \rangle \in \Gamma_f$ согласно определению g. Поднимая эту точку с Γ_f на 1-уровень F, найдем нужное значение y. В случае $\gamma = 1$ значения t, t_1 можно взять любыми.

Пусть $\gamma > 1$. Найдем тогда t из системы уравнений $\mathrm{Gd}(k, t) = f(x_1, \ldots, x_n, k)$ для всех $1 < k \leqslant \gamma - 1$. (Правые части существуют в силу определения $D(g)$.)

Наконец, при каждом $k \leqslant \gamma - 1$ поднимем точку

$\langle x_1, \ldots, x_n, k, \mathrm{Gd}(k, t) \rangle \in \Gamma_f$

до точки на $F = 1$ с дополнительной координатой $y^{(k)}$, после чего найдем t_1 из системы уравнений

$\mathrm{Gd}(k, t_1) = y^{(k)}, \quad 1 \leqslant k \leqslant \gamma - 1.$

Это обратит в единицу все сомножители в $\prod_{k=1}^{\gamma-1}$. В самом деле,

$s(\mathrm{Gd}(k, t)) = 1$, потому что

$\mathrm{Gd}(k, t) = f(x_1, \ldots, x_n, k) \geqslant 2$ при $k \leqslant \gamma - 1$; наконец,
$F_k = F(x_1, \ldots, x_n, k, \mathrm{Gd}(k, t), \mathrm{Gd}(k, t_1)) = 1$

по определению t, t_1.

4.11. Устойчивость относительно рекурсии. Нам осталось провести последний этап доказательства теоремы 4.3.

Пусть f, g — частичные функции от n, $n + 2$ переменных соответственно, а h — функция от $n + 1$ переменной, которая получается из них с помощью рекурсии:

$h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n),$
$h(x_1, \ldots, x_n, k + 1) = g(x_1, \ldots, x_n, k, h(x_1, \ldots, x_n, k)).$

Мы должны установить, что если Γ_f, Γ_g примитивно перечислимы, то и Γ_h примитивно перечислим.

Пусть F, G — примитивно рекурсивные функции, 1-уровни которых проектируются на Γ_f, Γ_g соответственно:

$\varphi = f(x_1, \ldots, x_n) \Leftrightarrow \exists y, \; F(x_1, \ldots, x_n, \varphi, y) = 1,$
$\gamma = g(x_1, \ldots, x_{n+2}) \Leftrightarrow \exists z, \; G(x_1, \ldots, x_{n+2}, \gamma, z) = 1$

(как в п. 4.10, достаточно ограничиться случаем, когда коразмерность проекции равна 1).

Построим явно функцию H, 1-уровень которой проектируется на Γ_h. Ее аргументами будут $x_1, \ldots, x_{n+1}, \eta, y, t, t_1$ (η — аргумент, который станет значением h). Положим

$\tilde{s}(1) = 1$, $\tilde{s}(x) = 2$ при $x \geqslant 2$;
$G_k = G(x_1, \ldots, x_n;\ k-1;\ \mathrm{Gd}(k-1, t),\ \mathrm{Gd}(k, t),\ \mathrm{Gd}(k, t_1))$,

$$H = F(x_1, \ldots, x_n; \mathrm{Gd}(1, t), y) \cdot \tilde{s}[(\eta - \mathrm{Gd}(x_{n+1}, t))^2 + 1] \prod_{k=2}^{x_{n+1}} G_k.$$

(Мы считаем, что $\prod_{k=2}^{x_{n+1}} = 1$, если $x_{n+1} = 1$.) Как в п. 4.10, легко проверяется, что H примитивно рекурсивна.

Включение $\mathrm{pr}(H = 1) \subset \Gamma_h$. Пусть $\langle x_1, \ldots, x_{n+1}, \eta, y, t, t_1 \rangle$ — точка на $H = 1$. Мы должны проверить, что $h(x_1, \ldots \ldots x_{n+1}) = \eta$.

Так как второй сомножитель $H = 1$, то получаем прежде всего $\eta = \mathrm{Gd}(x_{n+1}, t)$.

Если к тому же $x_{n+1} = 1$, то равенство единице первого сомножителя H дает с учетом предыдущего

$$\eta = \mathrm{Gd}(1, t) = f(x_1, \ldots, x_n) = h(x_1, \ldots, x_n, 1).$$

Пусть теперь $x_{n+1} > 1$. Тогда из равенства $G_k = 1$ при всех $2 \leqslant k \leqslant x_{n+1}$ находим

$$\mathrm{Gd}(k, t) = g(x_1, \ldots, x_n, k-1, \mathrm{Gd}(k-1, t)),$$

а из равенства $F = 1$ и определения h

$$\mathrm{Gd}(1, t) = f(x_1, \ldots, x_n) = h(x_1, \ldots, x_n, 1).$$

Поднимаясь по k от $k = 1$ до $k = x_{n+1}$ и пользуясь рекурсивным определением h, убеждаемся индукцией по k, что

$$\mathrm{Gd}(k, t) = h(x_1, \ldots, x_n, k)$$

и, в частности,

$$\eta = \mathrm{Gd}(x_{n+1}, t) = h(x_1, \ldots, x_{n+1}).$$

Включение $\Gamma_h \subseteq \mathrm{pr}(H = 1)$. Дана точка

$$\langle x_1, \ldots, x_{n+1}, \eta = h(x_1, \ldots, x_{n+1}) \rangle \in \Gamma_h.$$

Мы должны подобрать такие значения y, t, t_1, чтобы обратить H в 1.

Если $x_{n+1} = 1$, выберем t так, чтобы $\mathrm{Gd}(1, t) = h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n)$. После этого поднимем точку $\langle x_1, \ldots, x_n, \mathrm{Gd}(1, t) \rangle \in$

$\in \Gamma_f$ до точки $F = 1$; это дает нужное значение y; t_1 можно выбирать как угодно.

Пусть, наконец, $x_{n+1} > 1$. Сначала выберем t как решение системы уравнений

$$\mathrm{Gd}\,(1, t) = f(x_1, \ldots, x_n) = h(x_1, \ldots, x_n, 1),$$
$$\mathrm{Gd}\,(k, t) = h(x_1, \ldots, x_n, k) = g(x_1, \ldots, x_n, k-1, \mathrm{Gd}\,(k-1, t)),$$
$$2 \leqslant k \leqslant x_{n+1}.$$

Затем, подняв точку $\langle x_1, \ldots, x_n, \mathrm{Gd}\,(1, t)\rangle \in \Gamma_f$ на 1-уровень F, отыщем y. Это обратит в 1 первые два сомножителя H.

После этого поднимем точки

$$\langle x_1, \ldots, x_n, k-1, \mathrm{Gd}\,(k-1, t), \mathrm{Gd}\,(k, t)\rangle \in \Gamma_g, \quad 2 \leqslant k \leqslant x_{n+1}$$

на 1-уровень G, добавив координаты $z^{(k)}$ и решив относительно t_1 систему уравнений

$$\mathrm{Gd}\,(k, t_1) = z^{(k)}, \quad 2 \leqslant k \leqslant x_{n+1}.$$

Это обеспечит обращение в 1 сомножителей G_k.

Доказательство теоремы 4.3 окончено.

4.12. Объяснение термина «перечислимое множество».

Теорема 4.3 показывает, что если E перечислимо, то существует программа, «порождающая E» (ср. с п. 4.1) Действительно, пусть E — проекция на первые n координаты 1-уровня примитивно рекурсивной функции $f(x_1, \ldots, x_n, y)$. Порождающая E программа должна перебирать векторы $\langle x_1, \ldots, x_n, y\rangle$, скажем, в канторовском порядке, вычислять f и подавать на выход $\langle x_1, \ldots, x_n\rangle$ в том и только в том случае, когда $f = 1$ (ср со следствием 4.18). В отличие от «распознающей» программы типа описанной в § 1, которая может навечно застрять на элементе, не принадлежащем E, порождающая программа рано или поздно выпишет любой элемент E и ничего кроме него. Однако, если E пусто, мы этого можем никогда не узнать

В заключение параграфа обсудим свойства так называемых разрешимых множеств. Интуитивно $E \subseteq (Z^+)^n$ разрешимо, если есть программа, по каждому элементу $(Z^+)^n$ выясняющая, принадлежит ли он E или нет.

4.13. Определение. *Множество $E \subseteq (Z^+)^n$ называется разрешимым, если оно и его дополнение перечислимы.*

В § 5 и в следующей главе мы докажем, что существуют перечислимые, но не разрешимые множества. Этот результат тесно связан с теоремой Геделя о неполноте, которой посвящена гл. IV.

4.14. Теорема. *Следующие три класса множеств совпадают:*

а) *множества, характеристическая функция которых рекурсивна;*

б) *множества уровня общерекурсивных (всюду определенных частично рекурсивных) функций;*

в) *разрешимые множества.*

Доказательство. Соотношения а) = б) $\subset$ в) очевидны из уже доказанного. Поэтому остается проверить включение в) $\subset$ а).

Пусть $E \subseteq (Z^+)^n$ — разрешимое множество, E' — его дополнение. По определению

$$E = D(f), \quad E' = D(f')$$

для некоторых частично рекурсивных функций f, f'. Можно даже считать, что $f \equiv 1$, $f' \equiv 2$ (там, где они определены). Рассмотрим $\Gamma_f \cup \Gamma_{f'} \subseteq (Z^+)^n \times Z^+$. Очевидно, это объединение является графиком Γ_g характеристической функции g множества E. Из леммы 4.8 и дальнейшего обсуждения ясно, что Γ_g перечислим вместе с Γ_f и $\Gamma_{f'}$. Поэтому частичная рекурсивность g будет вытекать из следующего результата, который представляет самостоятельный интерес.

4.15. Предложение. *Для того чтобы частичная функция g из $(Z^+)^n$ в Z^+ была частично рекурсивной, необходимо и достаточно, чтобы ее график Γ_g был перечислим.*

Доказательство. Необходимость уже установлена.

Проверим достаточность. Так как Γ_g перечислим, существует такая примитивно рекурсивная функция

$$G(x_1, \ldots, x_n, y, z)$$

(см. п. 4.10), что Γ_g = проекция на $(x_1, \ldots, x_n, y)$ 1-уровня G. Положим

$$H = (x_1, \ldots, x_n, u) = G(x_1, \ldots, x_n, t_1^{(2)}(u), t_2^{(2)}(u)),$$

где $u \to \langle t_1^{(2)}(u), t_2^{(2)}(u)\rangle$ — примитивно рекурсивный изоморфизм $Z^+ \to (Z^+)^2$, описанный в п. 4.5 и 4.7. Очевидно, H примитивно рекурсивна. Наконец, положим

$$h(x_1, \ldots, x_n) = \min\{u \mid H(x_1, \ldots, x_n, u) = 1\}.$$

Это частично рекурсивная функция, область определения которой совпадает с $D(g)$ и которая, как легко видеть, позволяет вычислить g:

$$g(x_1, \ldots, x_n) = t_1^{(2)}(h(x_1, \ldots, x_n)).$$

Тем самым g частично рекурсивна, чем завершается доказательство предложения 4.15 и теоремы 4.14.

4.16. Следствие. *Для любой частично рекурсивной функции g существует описание, в котором операция μ применяется один раз.*

4.17. Следствие. *Если частично рекурсивная функция g всюду определена, то существует ее описание $g_1, \ldots, g_N = g$, в котором все функции всюду определены.*

Действительно, описание, конец которого (начиная с G) построен в п. 4.15, обладает этим свойством.

4.18. Следствие. *Класс перечислимых множеств совпадает с классом множеств значений примитивно рекурсивных отображений.*

Действительно: множество значений f есть проекция графика f. Наоборот, перечислимое множество $E \subset (Z^+)^n$, являющееся проекцией на $(x_1, \ldots, x_n)$-пространство 1-уровня примитивно рекурсивной функции $f(x_1, \ldots, x_n, y)$, совпадает с множеством значений примитивно рекурсивного отображения

$$g(z) = \begin{cases} \langle t_1^{(n+1)}(z), \ldots, t_n^{(n+1)}(z)\rangle, \text{ если } f\left(t_1^{(n+1)}(z), \ldots, t_n^{(n+1)}(z)\right) = 1, \\ g(z-1) \text{ в противном случае.} \end{cases}$$

4.19. Следствие. а) *Конечные множества и их дополнения в* $(Z^+)^n$ *разрешимы.*

б) *Любое частичное отображение из* $(Z^+)^m$ *в* $(Z^+)^n$ *с конечной областью определения рекурсивно и вычислимо.*

В самом деле, одноточечное множество $\{a\} \in Z^+$ есть уровень суммы двух подходящих ступенек, в дополнение к нему — другой уровень такой суммы. Конечные объединения и пересечения сохраняют разрешимость и дают а) для $n = 1$; изоформизм $\tau^{(n)}$ позволяет перенести этот результат на все n.

Отсюда следует и б), ибо графики рассматриваемых отображений конечны и, значит, перечислимы.

5. ЭЛЕМЕНТЫ РЕКУРСИВНОЙ ГЕОМЕТРИИ

5.1. Основные объекты современных геометрических дисциплин (дифференциальная, аналитическая, алгебраическая геометрии) определяются как пары <множество, совокупность частичных функций на нем>, удовлетворяющие тем или иным аксиомам. Это — новое воплощение старой идеи о том, что математика изучает «числа и фигуры».

Множества определения частичных функций рассматриваемого типа, как правило, открыты в подходящей топологии, а сами функции образуют на этой топологии пучок.

В этом параграфе мы прослеживаем аналогии между теорией рекурсивных функций и более классическими геометриями. Читатель, не знакомый с языком топологии и теории пучков, может пропускать упоминания о них и следить лишь за точными утверждениями о свойствах рекурсивных объектов.

Начнем с определений.

Пусть $E \subseteq (Z^+)^m$ — перечислимое множество. Рассмотрим структуру на E, образованную следующими данными:

а) $\mathscr{E} = \{E' \mid E' \subseteq E,\ E'$ перечислимо$\}$,

б) для каждого $E' \in \mathscr{E}$, $R(E') = \{f \mid D(f) = E', f: E' \to Z^+$ рекурсивна$\}$.

Положим $\mathscr{R}$ = множество пар $\langle E', R(E')\rangle$, $E' \in \mathscr{E}$.

Покажем, что структура $\{\mathscr{E}, \mathscr{R}\}$ во многом сходна со структурой «топологическое пространство с пучком». Это позволяет естественно истолковывать некоторые известные результаты о перечислимых множествах и ставить новые задачи, руководствуясь аналогией с другими геометрическими теориями.

Начнем со следующих простых замечаний.

5.2. *$\mathscr{E}$ является решеткой, т. е. замкнуто относительно конечных объединений и пересечений.*

Поскольку для произвольных бесконечных объединений это не так, $\mathscr{E}$ нельзя рассматривать как систему открытых подмножеств E в некоторой топологии. Тем не менее устойчивость относительно важного класса бесконечных объединений будет показана в п 5.9. Будем говорить, что $\mathscr{E}$ определяет *квазитопологию* на E (она обладает свойствами, близкими к свойствам так называемых топологий Гротендика, но не удовлетворяет всем аксиомам последних).

5.3. *Пусть $E', E'' \in \mathscr{E}$, $E' \subseteq E''$. Тогда ограничение функций определяет отображение*

$$R(E'') \to R(E') : f \to f|_{E'}$$

Действительно, пусть $c_{E'} \in R(E')$, $c_{E'} = 1$ на E'. Тогда $f|_{E'} = fc_{E'}$ рекурсивна вместе с f и $c_{E'}$.

5.4. *Пусть*

$$E' = \bigcup_{k=1}^{n} E_k, \quad E', E_k \in \mathscr{E}.$$

Пусть $f_k \in R(E_k)$ и f_k согласованы на пересечениях:

$$\forall\, i, j \leqslant n,\ f_i|_{E_i \cap E_j} = f_j|_{E_i \cap E_j}.$$

Тогда существует (очевидно, единственная) функция

$$f \in R(E'),\ \text{такая, что}\ \forall\, k \leqslant n,\ f|_{E_k} = f_k.$$

Нужно проверить только, что $f \in R(E')$, ибо существование $f : E' \to Z^+$, «склеенной» из f_k, очевидно. Но график f перечислим как объединение конечного числа перечислимых графиков

$$\Gamma_{fi} \subseteq E' \times Z^+,$$

и остается воспользоваться предложением 4.15.

Результаты п. 5.2 и 5.3 позволяют рассматривать $\mathscr{R}$ как *пучок* на квазитопологии $\mathscr{E}$.

5.5. *Пусть E_1, E_2 — перечислимые множества и $f : E_1 \to E_2$ рекурсивное отображение. Оно определяет морфизм соответствующих квазитопологий с пучками в следующем смысле:*

а) *Если $E' \subseteq E_2$ перечислимо, то $f^{-1}(E') \subseteq E_1$ перечислимо.*

б) *Композиция с f определяет для каждого $E' \subseteq E_2$ отображение*

$$f^*_{E'} : R(E') \to R(f^{-1}(E')).$$

Первая часть следует из того, что функция $c_{f^{-1}(E')} = c_{E'} \circ f$ рекурсивна вместе с $c_{E'}$ и f; вторая очевидна.

Могло бы создаться впечатление, что пара $\langle \mathscr{E}, \mathscr{R} \rangle$ достаточно полно характеризует E вне зависимости от вложения $E \subseteq (Z^+)^m$, однако это не так.

5.6. Предложение. *Пусть E_1, E_2 — бесконечные перечислимые множества. Тогда существует биекция $f : E_1 \tilde{\to} E_2$, такая, что f и f^{-1} рекурсивны. Она индуцирует изоморфизм $\langle \mathscr{E}_1, \mathscr{R}_1 \rangle \tilde{\to} \langle \mathscr{E}_2, \mathscr{R}_2 \rangle$.*

Доказательство. Установим следующие более точные факты:

а) Если $E \subseteq Z^+$ бесконечно и разрешимо, то существует общерекурсивная биекция $f : Z^+ \tilde{\to} E$ с рекурсивной f^{-1}, которая является возрастающей функцией. Верно и обратное.

б) Если $E \subseteq Z^+$ бесконечно и перечислимо, то существует общерекурсивная биекция $f : Z^+ \tilde{\to} E$ с рекурсивной f^{-1}.

Пусть сначала E разрешимо, $g(x) = 2$ при $x \in E$, $g(x) = 1$ при $x \notin E$, $h = c_E$. Положим

$$f(z) = \min \left\{ y \;\middle|\; \left(\sum_{x=1}^{y} g(x) - y - z \right)^2 + 1 = 1 \right\} = z\text{-й}$$

элемент E. Легко убедиться, что

$$f^{-1}(x) = \left(\sum_{y=1}^{x} g(y) - x \right) h(x) = \begin{cases} \text{номер } x \text{ как элемента } E, & \text{если } x \in E; \\ \text{не определена} & \text{иначе.} \end{cases}$$

Теперь пусть E перечислимо. Согласно следствию 4.18 существует примитивно рекурсивная функция $g : Z^+ \to E$, образ которой совпадает с E. Изменим ее так, чтобы она стала биекцией. Положим

$$F = \{k \in Z^+ \mid \forall\, i < k,\ g(i) \neq g(k)\}.$$

Это множество разрешимо: оно есть 1-уровень примитивно рекурсивной функции h:

$$h(1) = 1;\ h(k) = \prod_{i=1}^{k-1} s((g(i) - g(k))^2 + 1) \text{ для } k \geqslant 2,$$

$$s(x) = \begin{cases} 1 \text{ при } x \geqslant 2, \\ 2 \text{ при } x = 1. \end{cases}$$

Из предыдущего результата существует рекурсивная биекция $g' : Z^+ \tilde{\to} F$. Положим $f = g \circ g'$. Так, для $g|_F : F \tilde{\to} E$ есть биекция, то и $f : Z^+ \tilde{\to} E$ есть биекция. Обратная функция частично рекурсивна, ибо

$$f^{-1}(x) = \min \{y \mid (f(y) - x)^2 + 1 = 1\}.$$

Предложение доказано.

Имея в виду этот результат, вложение $E \subseteq (Z^+)^m$ обычно рассматривают как существенный элемент структуры E; в частности, E_1 и E_2 называются *изоморфными*, если существует биекция между ними, индуцированная рекурсивной биекцией объемлющих пространств.

Полная классификация перечислимых множеств с точностью до изоморфизма неизвестна, хотя многие тонкие результаты получены в теории сводимостей. Ниже, пользуясь теоремой, которая будет доказана в следующей главе, мы покажем только, что не все перечислимые множества разрешимы.

5.7. Семейства. Пусть $m \geqslant 0$, B — некоторое множество. Назовем *семейством* m-множеств (или *m-семейством*) *над базой* B любое отображение $B \to \mathcal{P}((Z^+)^m)$. Если $E_k \subseteq (Z^+)^m$ — образ $k \in B$ при этом отображении, то мы будем обозначать это семейство также $\{E_k\}$. Множество $E = \{\langle x, k\rangle \mid x \in E_k\} \subseteq (Z^+)^m \times B$ будем называть *тотальным пространством* семейства.

Аналогично отображение $B \to \{$частичные функции из $(Z^+)^m$ в $Z^+\}$ назовем *семейством m-функций над базой* B. Функцию $f : \langle x, k\rangle \to f_k(x)$ для $x \in D(f_k)$ назовем *тотальной функцией* семейства.

Семейство m-множеств (соответственно m-функций) назовем *перечислимым*, если $B \subseteq (Z^+)^m$ для некоторого n и тотальное пространство перечислимо в $(Z^+)^m \times (Z^+)^n$ (соответственно тотальная функция частично рекурсивна на $(Z^+)^m \times (Z^+)^n$.

Если $\{E_k\}$ перечислимо, то множество $\{k \in B \mid E_k$ не пусто$\}$ перечислимо как проекция тотального пространства E и все E_k перечислимы как пересечения
$E \cap (Z^+)^m \times \{k\}$.

Аналогично если $\{f_k\}$ перечислимо, то множество $\{k \in B \mid f_k$ — не пустая функция$\}$ перечислимо как проекция области определения тотальной функции f и все f_k частично рекурсивны как ограничения f на перечислимые множества $D(f) \cap (Z^+)^m \times \{k\}$.

Если $\{f_k\}$ — перечислимое семейство m-функций, то $\{D(f_k)\}$—перечислимое семейство m-множеств (с тотальным пространством $D(f)$), а $\{\Gamma_{f_k}\}$ — перечислимое семейство $(m+1)$ — множеств (с тотальным пространством Γ_f, точнее, результатом перестановки множителей в Γ_f).

Перечислимое семейство $\{E_k\}$ (соответственно $\{f_k\}$) называется *версальным*, если любое перечислимое m-множество (соответственно любая частично рекурсивная m-функция) содержится среди членов семейства. (Термин заимствован из современной геометрии; снята приставка «уни», указывающая в слове «универсальный» на однократность вхождения всех членов семейства).

В § 1 гл. III мы покажем, что для любого m версальные семейства *существуют*. Это — один из центральных результатов теории; тотальные пространства и функции версальных семейств являются исход-

ными для исследований неразрешимости и многих других важных конструкций.

Сейчас мы ограничимся простейшим и самым фундаментальным приложением.

5.8. Теорема. *Пусть $\{E_k\}$ — версальное семейство 1-множеств над базой $B \subseteq Z^+$. Тогда множество*

$$F = \{k \mid k \in E_k\}$$

перечислимо, но неразрешимо.

Доказательство. Пусть $E \subset Z^+ \times Z^+$ — тотальное пространство семейства. Тогда
$F =$ проекция на 1-й множитель $E \cap$ (диагональ в $Z^+ \times Z^+$) и потому перечислимо.

С другой стороны, для любого $k \in B$, $\bar{F} = Z^+ \cap F \neq E_k$, ибо k принадлежит либо $\bar{F}$, либо E_k, но не обоим множествам вместе. Так как $\{E_k\}$ — версальное семейство, то $\bar{F}$ не может быть перечислимым. Теорема доказана.

Покажем теперь, как использовать перечислимые семейства для усиления результатов п. 5.2 и 5.4. Вернемся к обозначениям начала этого параграфа.

5.9. *$\mathscr{E}$ замкнуто относительно объединения элементов любого перечислимого множества семейства подмножеств E.*

Действительно, пусть $\{E'_k\}$ — такое семейство, E' — его тотальное пространство, $E' \subseteq (Z^+)^m \times (Z^+)^n$. Тогда $\bigcup\limits_{k \in B} E_k =$ проекция E' на $(Z^+)^m$

5.10. *Пусть $\{f_k\}$ — перечислимое семейство частичных функций на E, $E'_k = D(f_k)$, $E' = \bigcup\limits_{k \in B} E'_k$ и $\forall i, j \in B$, $f_i|_{E'_i \cap E'_j} = f_j|_{E'_i \cap E'_j}$ Тогда существует единственная функция $f \in R(E')$, склеенная из f_i.*

Действительно, график Γ_f перечислим как объединение перечислимого семейства перечислимых множеств Γ_{f_k}.

Приведем в заключение несколько результатов о структуре $\mathscr{E}$. В силу предложения 5.6 достаточно ограничиться подмножествами Z^+.

5.11. Предложение. *Существуют перечислимые подмножества $F \subset Z^+$ с бесконечным дополнением, такие, что для любого бесконечного $E \in \mathscr{E}$ имеем $F \cap \mathscr{E} \neq \varnothing$, так что $F \cap E$ бесконечно.*

Такие F называются *простыми*; с точки зрения наших топологических представлений они подобны плотным открытым множествам.

Доказательство. Пусть $\{E_k\}$ — версальное семейство 1-множеств над Z^+ с тотальным пространством $E \subset Z^+ \times Z^+$. Положим $E' = E \cap \{\langle k, x\rangle \mid x > 2k\}$. Так как E' перечислимо, существует примитивно рекурсивное отображение с образом E':

$$g = (g_1, g_2) : Z^+ \to E'.$$

Положим $h(k) = \min\{z \mid g_1(z) = k\}$, $f(k) = g_2(h(k))$ и обозначим через F множество значений f. Дополнение к F бесконечно, ибо $f(k) > 2k$. Пересечение F с любым бесконечным E_k непусто, ибо все значения $g_2(z)$ при $g_1(z) = k$ лежат в $E_k \cap E' \neq \varnothing$.

Предложение доказано.

5.12. Предложение. а) *В фактор-решетке $\mathcal{E}/$(конечные множества) существуют нетривиальные максимальные элементы.*

б) *Любое непростое перечислимое множество с бесконечным дополнением содержится в таком элементе.*

в) *Существуют простые перечислимые множества с бесконечным дополнением, не содержащиеся в нетривиальном максимальном множестве.*

За доказательством этого и многих других результатов мы отсылаем к книге Роджерса [2].

6. КОНСТРУКТИВНЫЕ ОБЪЕКТЫ И АЛГОРИТМЫ

6.1. В этом параграфе мы кратко опишем те понятия теории вычислимости, в которых большой упор делается на реализацию процесса вычисления, а само вычисление понимается как детерминированная обработка данных, представленных не обязательно целыми числами.

Эти понятия возникают как конкретизация (в форме математических определений) нескольких интуитивных понятий:

а) универсума конструктивных объектов;

б) универсума предписаний по переработке конструктивных объектов, т. е. описаний алгоритмов;

в) универсума устройств, способных реализовать работу алгоритмов;

г) универсума процессов работы этих устройств.

Разберём эти понятия по очереди.

6.2. К о н с т р у к т и в н ы е о б ъ е к т ы. Каждый конструктивный универсум представляет собой конечное или счетное множество объектов, допускающих финитное описание в некотором языке. Чтобы превратить это представление в математическое определение, конструктивные объекты часто отождествляют с этими описаниями. Вот примеры.

а. Целые числа как конструктивные объекты можно представлять себе в виде наборов палочек: I, II, III, IIII ..., которые изображают соответственно 1, 2, 3, 4 ... Конечные последовательности целых чисел можно представлять наборами таких палочек, разделенными нулями.

б. Если задан конечный алфавит A, слова в этом алфавите, т. е. конечные последовательности букв из A, являются конструктивными объектами.

в. Можно объявить, что в качестве универсума конструктивных объектов выбираются конечные неориентированные графы. При этом подразумевается, что квалифицированный читатель сам вообразит се-

бе несложный формальный язык, такой, что явно описываемые слова в этом языке будут отвечать таким графам. Еще один пример: объединение первых этажей теоретико-множественного универсума V в конечном или счетном числе (см. Д и ДН, с. 101) является конструктивным универсумом. Он состоит из конечных множеств, элементами которых являются конечные множества, и замкнут относительно операций объединения, конструкции пар, перехода к множеству подмножеств и т. п.

6.3. Описания алгоритмов. Данному в п. 2.2 определению функции $\text{рг}_i^n : (Z^+)^n \to Z^+$ может отвечать примерно такое описание алгоритма, который перерабатывает последовательности палочек, разделенных n нулями, в последовательности палочек.

а) В предъявленной последовательности найдите $(i-1)$-й слева нуль и i-й слева нуль.

б) Сотрите все знаки, находящиеся левее $(i-1)$-го нуля (включая его) и правее i-го нуля (включая его). Аналогичные рецепты можно дать для вычисления остальных простейших функций из § 2. Элементарные операции над простейшими функциями сводятся к соединению описаний алгоритмов, вставлению цикла и т. п.

Степень подробности, с которой должно быть составлено описание алгоритма, и степень формализованности языка описания, очевидно, зависят от структуры устройства, которое будет выполнять алгоритм. Человеку может хватить нескольких неформальных указаний, ЭВМ должна получить не просто формально правильный текст, но даже физически правильно реализованный текст (в виде колоды перфокарт с жесткими допусками на размеры и прочность самих карт и пробитых в них отверстий).

Очень важно, что формализованные описания алгоритмов сами могут рассматриваться как конструктивные объекты и, в частности, подвергаться переработке в ходе вычисления (см. гл. IV).

6.4. Вычисляющие устройства. Эти устройства должны реализовать некоторые элементарные операции над конструктивными объектами («добавлять и стирать палочки») и логические операции, предусмотренные описанием алгоритмов, состоящие в выборе очередного действия. Детальный анализ одного из наиболее экономных наборов элементарных шагов был впервые проведен Тьюрингом в знаменитой работе, ставшей провозвестницей нынешней эпохи компьютеров. Мы не будем воспроизводить здесь описания «машины Тьюринга», которое читатель сможет найти во многих книгах (см., например, [6—9]).

Подчеркнем снова, что вычисляющее устройство (в разумной идеализации) может быть описано конечным текстом и потому снова может рассматриваться как конструктивный объект. Но обычно в описании «устройства» отделяют переменную программную часть от неизменяющегося «железа». Универсум вычисляющих устройств может

появиться при исследовании системы взаимодействующих автоматов.

6.5. Связь с рекурсивными функциями. Чтобы связать эти представления с теорией рекурсивных функций, используют стандартный прием: нумерацию всех встречающихся универсумов целыми числами. Экспериментальный факт, который можно считать дополнением к тезису Черча, состоит в том, что всегда существуют простые и естественные нумерации, после применения которых все представления о вычислимости адекватно переводятся на язык рекурсивности. В IV гл. мы изложим некоторые результаты математической теории нумерации, которые оправдывают принятия точки зрения, что теория алгоритмической *вычислимости* без потерь сводится к теории рекурсивной вычислимости. Но, как мы уже отмечали, это не относится к теории алгоритмических *вычислений* с ее проблемами минимизации числа действий, объема памяти, задачами исследования топологии вычислительных процессов (возможности параллельного вычисления) и т. п.

Глава II

ДИОФАНТОВЫ МНОЖЕСТВА И АЛГОРИТМИЧЕСКАЯ НЕРАЗРЕШИМОСТЬ

1. ОСНОВНЫЕ РЕЗУЛЬТАТЫ

1.1. В § 4 гл. I было доказано, что перечислимые множества суть проекции множеств уровня примитивно рекурсивных функций. Среди последних содержатся многочлены с коэффициентами из Z^+; назовем проекции их уровней *диофантовыми множествами*; этот класс не расширится, если разрешить коэффициентам лежать в Z. Основная цель этой главы — доказать следующий тонкий результат.

1.2. **Теорема.** *Перечислимые множества диофантовы, следовательно, эти два класса множеств совпадают.*

В § 2 описан план доказательства. Ажурные, хотя и совершенно элементарные конструкции, составляющие само доказательство, содержатся в § 3—7; читатель может их опустить без ущерба для понимания дальнейшего.

В § 1 гл. III на основе теоремы 1.2 будет установлено существование версальных семейств перечислимых множеств и функций; в § 5 гл. I было показано, как из этого следует существование неразрешимых перечислимых множеств.

В гл. IV будет существенно использоваться следствие из теоремы 1.2: *перечислимые множества выразимы в языке* L_1 Ar (см. Д и НД). Действительно, диофантовы множества по самому их определению выражаются формулами $\exists x_1 \ldots \exists x_n\,(p)$, где p — атомарная формула.

Оставшаяся часть этого параграфа посвящена описанию самых эффективных приложений теоремы 1.2: решение десятой проблемы Гильберта, конструкция многочленов, принимающих только (и все) простые значения и Z^+ и т. п.

1.3. Десятая проблема Гильберта. Гильберт сформулировал ее так: «Пусть задано диофантово уравнение с произвольными неизвестными и целыми рациональными числовыми коэффициентами. Указать способ, при помощи которого возможно после конечного числа операций установить, разрешимо ли это уравнение в целых рациональных числах».

Покажем, что из объединения теоремы 1.2, выводимой из нее теоремы 5.8 гл. I и тезиса Черча вытекает неразрешимость этой проблемы.

Прежде всего любое натуральное число есть сумма четырех квадратов целых чисел (Лагранж). Поэтому разрешимость уравнения $f(x_1, \ldots, x_n) = 0$ в $(Z^+)^n$ равносильна разрешимости уравнения $f(1 + \sum_{i=1}^{4} y_{i1}^2, \ldots, 1 + \sum_{i=1}^{4} y_{in}^2) = 0$ в $(Z)^{4n}$. Следовательно, достаточно установить алгоритмическую неразрешимость массовой проблемы «распознавание наличия решений в $(Z^+)^n$» (см. п. 2.6 гл. 1).

Пусть $E \subset Z^+$ — перечислимое, но не разрешимое множество. Представим его в виде проекции на t — координату 0-уровня многочлена $f_t = f(t; x_1, \ldots, x_n) = 0$, $f \in Z[t, x_1, \ldots, x_n]$. Уравнение $f_{t_0} = 0$; $t_0 \in Z^+$ разрешимо, если и только если $t_0 \in E$. Согласно обсуждению в § 2 гл. V соответствующая массовая проблема для семейства $\{f_t\}$ алгоритмически разрешима, если и только если характеристическая функция E вычислима. Но по выбору E она только полувычислима.

Таким образом, разрешимость в целых числах нераспознаваема уже для подходящего однопараметрического семейства уравнений. Число неизвестных в нем (и вообще коразмерность проекции, подразумеваемой в теореме 1.2) может быть сведено до 9 (Ю. В. Матиясевич). Точный минимум неизвестен, хотя очень интересен.

Подчеркнем, наконец, что конструкция диофантова представления любого перечислимого множества E совершенно эффективна в том смысле, что по заданному рекурсивному описанию функции f с $D(f) = E$ либо функции g с $g(Z^+) = E$ соответствующий многочлен может быть выписан явно. То же относится к построению версального семейства, перечислимого неразрешимого множества и т. д. Все это — конструктивные утверждения, а не просто теоремы существования.

1.4. Многочлен, представляющий простые числа. Поиски «явных формул» для простых чисел были традиционным предметом занятий бескорыстных любителей теории чисел в продолжение долгого времени. Эйлер указал многочлен $x^2 + x + 41$, принимающий длинный ряд только простых значений. Но давно было известно, что множество значений многочлена f из $Z[x_1, \ldots, x_n]$ в

целых точках не может состоять лишь из простых чисел, например, потому, что если p, q два достаточно больших простых числа, то сравнение $f \equiv 0 \bmod pq$ разрешимо (бесконечно многими способами). С другой стороны, в классе примитивно-рекурсивных функций задача уже решается: функция $\{i \to i\text{-е простое число}\}$ сама примитивно рекурсивна (ср. с § 1 гл. IV), но по тривиальным причинам.

Нетривиальная постановка вопроса и его решение снова связаны с теоремой 1.2: множество простых чисел есть множество всех положительных значений некоторого многочлена с целыми коэффициентами в точках из $(Z^+)^n$ (или, если угодно, из $(Z)^{4n}$: ср. редукцию в п. 1.3). Один из возможных многочленов явно выписан в § 8 этой главы.

Специфика простых чисел в этом общем результате никак не участвует:

1.5. Предложение. *Пусть $E \subseteq Z^+$ — диофантово множество. Тогда существует такой многочлен $g \in Z[x_0, \ldots, x_n]$, что E совпадает с множеством положительных значений g в точках из $(Z^+)^{n+1}$*

Доказательство. Пусть E — проекция на x_0-координату 0-уровня многочлена $f(x_0, x_1, \ldots, x_n)$. Положим

$$g = x_0[1 - f^2(x_0, x_1, \ldots, x_n)].$$

Ясно, что положительные значения g — это в точности элементы E.

Остается воспользоваться тем, что множество простых чисел разрешимо и потому диофантово в силу теоремы 1.2.

Множествами натуральных значений многочленов являются также:

1.6. *Последовательности* $\{1, 10, 100, \ldots, 10^k, \ldots\}$ или $\{1, 2^2, 3^{3^3}, \ldots, n^{n^{\cdot^{\cdot^{\cdot^n}}}}$ (n раз), $\ldots\}$.

Удивительно, как значения соответствующего многочлена проваливаются до нуля и ниже в окрестностях точек, где они так огромны.

1.7. *Множество Ферма*

$$\{n \mid n > 2 \text{ и } x^n + y^n + z^n = 0$$

разрешимо в $Z\}$. Таким образом, переменную n можно из экспоненты перевести в коэффициенты диофантова уравнения.

1.8. *Множество* $\{10\mathscr{E}_1, 10^2\mathscr{E}_2, \ldots, 10^n\mathscr{E}_n, \ldots\}$, где $\mathscr{E}_i$ — i-я после запятой цифра десятичного разложения e (или π, или $\sqrt[3]{2}$, или любого другого «вычислимого» иррационального числа).

1.9. *Множество всех неполных частных e или π, или $\sqrt[3]{2}$ при разложении в непрерывную дробь.*

Напомним, что для $\sqrt[3]{2}$ до сих пор неизвестно даже, конечно или бесконечно это множество.

Эти примеры показывают, что к задачам о разрешимости диофантовых уравнений сводятся многие теоретико-числовые вопросы. В гл. IV мы убедимся, что в некотором смысле слова к ним сводится вообще «почти вся математика».

2. ПЛАН ДОКАЗАТЕЛЬСТВА

2.1. В этом параграфе введены некоторые вспомогательные понятия и описан план доказательства теоремы 1.2.

Временно введен класс множеств, промежуточный между перечислимыми и диофантовыми. Чтобы определить его, рассмотрим отображение, которое ставит в соответствие каждому подмножеству $E \subseteq (Z^+)^n$ новое подмножество $F \subseteq (Z^+)^n$ по следующему правилу:

$$\langle x_1, \ldots, x_n \rangle \in F \Leftrightarrow \forall\, k \in [1, x_n],$$
$$\langle x_1, \ldots, x_{n-1}, k \rangle \in E.$$

Мы будем говорить, что F получилось из E применением ограниченного квантора общности по n-й координате. Аналогично определяется применение по любой координате.

2.2. Определение—лемма. *Рассмотрим следующие три класса подмножеств в $(Z^+)^n$ при всевозможных n.*

I. *Проекции множеств уровня примитивно-рекурсивных функций.*

II. *Наименьший класс множеств, содержащий множества уровня многочленов с целыми коэффициентами и замкнутый относительно операций конечного прямого произведения, конечного объединения, конечного пересечения, проекции и ограниченного квантора общности.*

III. *Проекции множеств уровня многочленов с целыми коэффициентами.*

Тогда справедливы следующие утверждения:

а) Класс I *совпадает с классом перечислимых множеств, а* III *— с классом диофантовых множеств.*

Множества класса II *будем называть D-множествами.*

б) $\mathrm{I} \supset \mathrm{II} \supset \mathrm{III}$.

Доказательство. а) Совпадение примитивно перечислимых множеств с перечислимыми было установлено в теореме 4.3 гл. I. Остальное — определения.

б) Не совсем очевидно только включение $\mathrm{II} \subset \mathrm{I}$. Прежде всего множество m-уровня многочлена f является множеством 1-уровня примитивно-рекурсивной функции $(f - m)^2 + 1$. Поэтому для проверки включения $\mathrm{II} \supset \mathrm{I}$ достаточно установить, что класс I замкнут относительно операций прямого произведения, объединения, пересечения (все в конечном числе и ограниченного квантора общности. Кроме последнего, все это установлено в лемме 4.8 гл. I.

Наконец, пусть примитивно перечислимое множество F является образом E относительно ограниченного квантора общности:

$$\langle x_1, \ldots, x_{n-1}, x_n \rangle \in F \Leftrightarrow \forall\, k \leqslant x_n,$$
$$\langle x_1, \ldots, x_{n-1}, k \rangle \in E.$$

Мы хотим построить по функции $f(x_1, \ldots, x_{n-1}; y_1, \ldots, y_m)$, 1-уровень которой проектируется на E, новую примитивно рекурсивную функцию g, 1-уровень которой будет проектироваться на F.

Естественная мысль — рассмотреть в качестве приближения к g произведение

$$\prod_{k=1}^{x_n} f(x_1, \ldots, x_{n-1}, k; y_{1k}, \ldots, y_{mk}),$$

где (y_{ik}) — «независимые переменные». Неприятное обстоятельство состоит в том, что число аргументов этой «функции» растет вместе с x_n. Чтобы справиться с этим, применим функцию Геделя $\mathrm{Gd}(k, t)$, определенную в п. 4.9 гл. V. Функция g будет зависеть от $x_1, \ldots, x_n$ и m дополнительных аргументов $t_1, \ldots, t_m$.

$$g(x_1, \ldots, x_n; t_1, \ldots, t_m) = \prod_{k=1}^{x_n} f(x_1, \ldots, x_{n-1}, k; \mathrm{Gd}(k, t_1), \ldots, \mathrm{Gd}(k, m)).$$

Она примитивно рекурсивна, потому что k-й сомножитель получается из f и Gd подстановкой и отождествлением аргументов, а затем g строится по этому сомножителю рекурсией.

Проверим, что множество F является проекцией 1-уровня функции g на $\langle x_1, \ldots, x_n\rangle$-координаты.

Действительно, если $g(x_1, \ldots, t_m) = 1$, то для всех $1 \leqslant k \leqslant x_n$ имеем

$$f(x_1, \ldots, k, \ldots, \mathrm{Gd}(k, t_m)) = 1,$$

т. е. для всех $1 \leqslant k \leqslant x_n$ точка $\langle x_1, \ldots, x_{n-1}, k\rangle$ принадлежит E Это значит, что $\langle x_1, \ldots, x_n\rangle \in F$.

Наоборот, если $\langle x_1, \ldots, x_n\rangle \in F$, мы можем поднять точку $\langle x_1, \ldots, x_{n-1}, k\rangle$, $1 \leqslant k \leqslant x_n$, на 1-уровень f. Пусть y-координаты этой точки будут $y_{1,k}, \ldots, y_{m,k}$.

Решим систему уравнений относительно t_i.

$\mathrm{Gd}(k, t_i) = y_{i,k}$ для всех $1 \leqslant k \leqslant x_n$. Это возможно по основному свойству Gd. Найденные значения аргументов t_i вместе с $x_1, \ldots, x_n$ обращают g в единицу. Это заканчивает доказательство леммы 2.2.

2.3. Дальнейший план работы следующий.

В § 3 показано совпадение классов I и II, в § 4—7 — совпадение классов II и III.

2.4. Замечания. По ходу доказательства леммы 2.2 мы получили следующие простые факты, которые следует постоянно иметь в виду:

а) В определениях классов I—III всюду можно заменить множества уровней на множества 1-уровней (перейдя от f к $(f - m)^2 + 1$).

б) Все классы I—III замкнуты относительно операций произведений, пересечений, объединений (все в конечном числе) и проекции. (Доказательство этого для класса I в лемме 4.8 гл. V применимо и к классу III).

Ограниченный квантор общности доставляет значительно большие трудности. На самом деле, замкнутости класса диофантовых множеств

относительно него посвящена наиболее техническая часть доказательства в § 4—7.

3. ПЕРЕЧИСЛИМЫЕ МНОЖЕСТВА ЯВЛЯЮТСЯ D-МНОЖЕСТВАМИ

Пусть $f : (Z^+)^n \to Z^+$ — примитивно-рекурсивная функция. Ее 1-уровень можно представить в виде проекции на первые n координат множества $\Gamma_f \cap | (Z^+)^n \times \{1\} |$, где Γ_f — график f. Поэтому любое перечислимое множество можно получить в виде проекции пересечения графиков двух примитивно-рекурсивных функций. Так как класс D-множеств замкнут относительно проекций и пересечений по определению, то для доказательства утверждения, вынесенного в заголовок, достаточно установить следующий факт.

3.1. Предложение. *Графики примитивно-рекурсивных функций являются D-множествами.*

Доказательство. Графики простейших функций диофантовы. Устойчивость свойства графиков «быть D-множествами» относительно композиции и соединения функций проверяется тем же рассуждением, что и в доказательстве леммы 4.8 гл. V.

Остается разобраться с рекурсией. Конечно, нам понадобятся сведения о графике функции Геделя. Здесь удобнее пользоваться gd вместо Gd.

3.2. **Лемма.** *График функции Геделя*

$$\mathrm{gd}\,(u, k, t) = \mathrm{rem}\,(1 + kt, u)$$

является диофантовым и тем более D-множеством.

Доказательство. Множество

$\Gamma_{\mathrm{gd}} = \{<u, k, t, \gamma> \mid \gamma =$ остаток от деления u на $1 + kt\}$ является пересечением следующих двух множеств в $(Z^+)^4$:

E_1: $\gamma \leqslant 1 + kt$, $\qquad E_2 : u - \gamma \geqslant 0$ и делится на $1 + kt$.

Оба они диофантовы. Действительно, E_1 есть проекция множества 0-уровня многочлена $2 + kt - \gamma - y_1$, E_2 — проекция множества 0-уровня многочлена $u - \gamma - (1 + kt)(y_2 - 1)$.

Лемма доказана.

3.3. Следствие. *Пусть f, g — функции от n и $n + 2$ аргументов, графики которых являются D-множествами. Тогда D-множества определяют следующие уравнения:*

$$E : \mathrm{gd}\,(u, 1, t) = f\,(x_1, \ldots, x_n),$$
$$F : \mathrm{gd}\,(u, x_{n+1} + 1, t) = g\,(x_1, \ldots, x_{n+1}, \mathrm{gd}\,(u, x_{n+1}, t))$$

в пространствах $(x_1, \ldots, x_{n+1}, u, t \ldots)$ (где многоточием обозначены любые дополнительные координаты).

Доказательство. Введение лишних координат сводится к прямому умножению на $(Z^+)^p$, которое, конечно, переводит D-множества в D-множества.

E можно представить в виде проекции пересечения множеств $\mathrm{gd}(u, k, t) = w$, $f(x_1, \ldots, x_n) = w$, $k = 1$ (k, w — вспомогательные координаты). Так как Γ_{gd} и Γ_f суть D-множества, то же верно для E.

Аналогично F можно представить в виде проекции пересечения множеств

$$\mathrm{gd}(u, x_{n+1} + 1, t) = w_1,$$

$$\mathrm{gd}(u, x_{n+1}, t) = w_2,$$

$$g(x_1, \ldots, x_{n+1}, w_2) = w_1.$$

Они являются D-множествами вместе с Γ_g и Γ_{gd}.

3.4. Доказательство предложения 3.1. Напомним, что нам осталось проверить следующее утверждение.

Даны функции f, g, как в следствии 3.3. Функция h определяется по ним рекурсией:

$$h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n),$$
$$h(x_1, \ldots, x_n, k + 1) = g(x_1, \ldots, x_n, k, h(x_1, \ldots, x_n, k)).$$

Тогда график Γ_h

$$\langle x_1, \ldots, x_{n+1}, \eta \rangle \in \Gamma_h \Longleftrightarrow \eta = h(x_1, \ldots, x_{n+1})$$

является D-миожеством вместе с графиками Γ_f и Γ_g.

Первый шаг. Положим $\Gamma_h = \Gamma^1 \cup \Gamma^2$, где $x_{n+1} = 1$ на Γ^1, $x_{n+1} \geqslant 2$ на Γ^2. Так как

$$\langle x_1, \ldots, x_{n+1}, \eta \rangle \in \Gamma^1 \Longleftrightarrow \{x_{n+1} = 1\},$$
$$\{\eta = f(x_1, \ldots, x_n)\},$$

то Γ^1 есть пересечение Γ_f и D-множества и потому является D-множеством. Остается проверить, что Γ^2 — тоже D-множество.

Второй шаг. В пространстве с координатами $\langle x_1, \ldots, x_{n+1}, \eta, u, t \rangle$ рассмотрим множества

$$E_1 : \eta = \mathrm{gd}(u, x_{n+1}, t),$$
$$E_2 : \mathrm{gd}(u, 1, t) = f(x_1, \ldots, x_n),$$
$$E_3 : x_{n+1} > 1,\ \mathrm{gd}(u, k, t) = g(x_1, \ldots, x_n, k - 1, \mathrm{gd}(u, k - 1, t))$$

для всех $2 \leqslant k \leqslant x_{n+1}$.

Легко проверить, что $\Gamma^2 = \mathrm{pr} \bigcap_{i=1}^{3} E_i$.

Как в § 4 гл. V, включение в одну сторону получается сравнением E_2, E_3 с индуктивным определением h, а в другую — подбором параметров u, t в функции Геделя.

Поэтому остается проверить, что E_i суть D-множества.

Третий шаг. E_1 есть график gd с лишними координатами; E_2 разобрано в следствии 3.3.

Наконец, E_3 «почти» получается из множества F, описанного в следствии 5.3, применением ограниченного квантора общности по координате x_{n+1}. Точнее (не обращая внимания на координату η, для сокращения записи):

$\langle x_1, \ldots, x_{n+1}, u, t\rangle \in E_3 \leftrightarrow \forall k \in [2, x_{n+1}]$,

$\langle x_1, \ldots, x_n, k-1, u, t\rangle \in F \leftrightarrow \forall k \in [1, x_{n+1}-1]$,

$\langle x_1, \ldots, x_n, k, u, t\rangle \in F$.

Следовательно, применяя к F ограниченный квантор общности по x_{n+1}, мы приходим к D-множеству, которое получается из E_3 уменьшением x_{n+1}-координаты всех точек E_3 на 1. Поэтому остается убедиться, что операция обратного сдвига на 1 сохраняет свойство «быть D-множеством», что легко следует из определений. Доказательство закончено.

4. РЕДУКЦИЯ

4.1. Ближайшие три параграфа посвящены доказательству того что класс D-множеств совпадает с классом диофантовых множеств. Как было замечено в конце § 2, для этого достаточно проверить, что класс диофантовых множеств замкнут относительно ограниченного квантора общности.

Пусть $f(x_1, \ldots, x_n, k, y_1, \ldots, y_m)$ — некоторый непостоянный многочлен с целыми коэффициентами. Он считается фиксированным до конца этого параграфа. Пусть d — его степень, C — сумма модулей коэффициентов.

Определим множество E из условия

$\langle x_1, \ldots, x_n, y\rangle \in E \leftrightarrow \forall k \leqslant y\, \exists \langle y_1, \ldots, y_m\rangle$,

$f(x_1, \ldots, x_n, k, y_1, \ldots, y_m) = 0$.

Мы хотим установить, что E *диофантово* (для любого выбора f). В этом параграфе доказан следующий редукционный результат.

4.2. Предложение. *E диофантово, если диофантовы следующие три множества:*

$x_1 = x_2^{x_3}$;

$x_1 = x_2!$;

$\dfrac{x_1}{x_2} = \binom{x_3/x_4}{x_5}$, $x_3 \geqslant x_4\, x_5$,

где $\binom{n}{k} = \dfrac{n(n-1)\ldots(n-k+1)}{k!}$ — *«биномиальный коэффициент»*.

Доказательство этого и всех последующих предложений такого типа строятся по единой схеме. Чтобы установить диофантовость E, введем вспомогательные множества E_i со следующими свойствами:

а) E = проекция $\bigcap_{i=1}^{N} E_i$,

б) E_i диофантовы.

Обычно, однако, непосредственно установить диофантовость всех E_i не удается, и к некоторым из них применяется аналогичная процедура. Таким образом, схема полного доказательства является деревом.

Литературное оформление каждого шага состоит из следующих этапов: введение вспомогательных переменных, пропадающих при проекции; конструкция множеств E_i с помощью явных соотношений; доказательство включения $E \subseteq \mathrm{pr} \bigcap_{i=1}^{N} E_i$ доказательство включения $E \supseteq \mathrm{pr} \bigcap_{i=1}^{N} E_i$.

4.3. Доказательство предложения 4.2. Вспомогательные переменные обозначим символами Y, N, K, Y_1, ..., Y_m. Множества E_i в пространстве

$$\langle x_1, \ldots, x_n, y, Y, N, K, Y_1, \ldots, Y_m \rangle$$

введем следующими соотношениями:

$E_1 : N \geqslant C(x_1, \ldots, x_n y Y)^d$,

$Y < Y_1, \ldots, Y < Y_m$

(содержательный смысл правой части первого неравенства — грубая оценка для значения многочлена f в точке $\langle x_1, \ldots, x_n, y, y_1, \ldots, y_m \rangle$, если $y, y_i < Y$),

$$E_2 : 1 + KN! = \prod_{k=1}^{y} (1 + kN!)$$

(это — «большой модуль»; равенство f нулю будет заменено делимостью на него.)

$$E_3 : f(x_1, \ldots, x_n, K, Y_1, \ldots, Y_m) \equiv 0 \bmod 1 + KN!,$$

$$E_{3+i} : \prod_{j \leqslant Y} (Y_i - j) \equiv 0 \bmod (1 + KN!),$$

$i = 1, \ldots, m$.

Множество E' определяется как $\bigcap_{i=1}^{m+3} K_i$.

Доказательство включения $E \subseteq \mathrm{pr}\, E'$.

Дана точка $\langle x_1, \ldots, x_n, y \rangle \in E$; мы должны подобрать значения остальных координат так, чтобы выполнялись соотношения $E_1, \ldots, E_{m+3}$.

Согласно определению E каждую точку $\langle x_1, \ldots, x_n, k \rangle$, $k \leqslant y$, можно поднять до 0-уровня f:

$$f(x_1, \ldots, x_n, k, y_{1k}, \ldots, y_{mk}) = 0.$$

Возьмем в качестве Y максимум y, y_{ik}. Затем, как и выше, отыщем Y_i и N, решая систему уравнений Геделя $\text{gd}(Y_i, k, N!) = y_{ik}$ для всех $1 \leqslant k \leqslant y$.

Доказательство леммы Геделя показывает, что Y_i, N можно взять как угодно большими, в частности, удовлетворив E_1. Число K однозначно определится из E_2.

Все выборы уже произведены. Соотношение E_{3+i} выполняется потому, что среди чисел $Y_i - j$ при $j \leqslant Y$ для каждого $k \leqslant y$ найдется

$$Y_i - y_{ik} \equiv 0 \bmod (1 + kN!)$$

по определению Y_i и gd. Следовательно, произведение слева в E_{3+i} делится на все $1 + kN!$, $1 \leqslant k \leqslant y$, которые попарно взаимно простые, ибо $N \geqslant y$ по E_1. Таким образом, это произведение делится на $1 + KN!$

Наконец, для проверки E_3 заметим, что из E_2 вытекает сравнение $K \equiv k \bmod (1 + kN!)$, $1 \leqslant k \leqslant y$, потому что $(1 + KN!) - (1 + kN!) \equiv 0 \bmod (1 + kN!)$ Но тогда, учитывая, что $y_{ik} \equiv Y_i \bmod (1 + kN!)$ по выбору Y_i, находим

$$f(x_1, \ldots, x_n, K; Y_1, \ldots, Y_m) \equiv f(x_1, \ldots, x_n, k, y_{1k}, \ldots, y_{mk}) \equiv 0 \bmod (1 + kN!).$$

Отсюда следует E_3 в силу попарной взаимной простоты модулей $1 + kN!$

Доказательство включения $\text{pr}\, E' \subseteq E$. Дана точка $\langle x_1, \ldots x_n, y, Y, N, K, Y_1, \ldots, Y_m \rangle$, координаты которой удовлетворяют соотношениям $E_1, \ldots, E_{m+3}$. Мы должны подобрать для каждого $k \leqslant y$ такой вектор $\langle y_{1k}, \ldots, y_{mk} \rangle$, чтобы

$$f(x_1, \ldots, x_n, k, y_{1k}, \ldots, y_{mk}) = 0.$$

С этой целью обозначим через p_k любой простой делитель числа $1 + kN!$ и положим

$y_{ik} =$ *остаток от деления* Y_i на p_k.

Покажем, что этот выбор дает требуемое.

Из E_3 следует, что

$$f(x_1, \ldots, x_n, k, y_{1k}, \ldots, y_{mk}) \equiv 0 \ (p_k).$$

Остается проверить, что число в левой части сравнения меньше p_k. Имеем:

p_k делит $\prod_{j \leqslant Y} (Y_i - j)$ в силу $E_{3+i} \Rightarrow p_k$ делит $Y_i - j$ для некоторого $j \leqslant Y \leqslant y_{ik} =$ остаток от деления Y_i на $p_k \leqslant Y \Rightarrow f(x_1, \ldots, x_n, k, y_{1k}, \ldots, y_{mk}) \leqslant C(x_1, \ldots, x_n y Y)^d \leqslant N < p_k$

(предпоследнее неравенство следует из E_1, а последнее из того, что p_k делит $1 + kN!$).

Окончание доказательства. Остается проверить, что диофантовость множеств $E_1, \ldots, E_{m+3}$ следует из диофантовости множеств, описанных в предложении 6.1.

Действительно, тривиальное введение вспомогательных переменных (для подстановок) позволяет свести проверку диофантовости всех E_i сначала к диофантовости множеств

$$x_1 = x_2!;$$

$$x_1 = \prod_{k \leqslant x_2} (1 + kx_3);$$

$$x_1 = \prod_{j \leqslant x_3} (x_2 - j), \quad x_2 > x_3.$$

После этого остается заметить, что второе из этих соотношений можно представить в виде

$$x_1 = x_3^{x_3}\, x_2! \binom{1/x_3 + x_2}{x_2},$$

а третье — в виде

$$x_1 = x_3! \binom{x_2 - 1}{x_3}, \quad x_2 > x_3.$$

Предложение 4.2 этим доказано.

5. КОНСТРУКЦИЯ СПЕЦИАЛЬНОГО ДИОФАНТОВА МНОЖЕСТВА

5.1. В этом параграфе мы начнем доказательство диофантовости множеств, введенных в предложении 4.2. Чтобы лучше уяснить ход доказательства, укажем, что самое существенное препятствие — быстрый рост одной из координат по сравнению с другими (например, $x_1 = x_2!$). Дж. Робинсон принадлежит важная идея: она показала, как из диофантовости любого конкретного множества в $(Z^+)^2$, одна из координат которого растет быстрее любой степени другой, но медленнее x^x (например, как экспонента), можно ввести диофантовость всех перечислимых множеств. После этого Матиясевичу и независимо Чудновскому удалось установить диофантовость множества такого типа, связанного с числами Фибоначчи. Историю вопроса см. в статье Ю. В. Матиясевича [18].

В этом параграфе приведена конструкция из более поздней статьи Ю. Матиясевича и Дж. Робинсон, являющаяся усовершенствованным вариантом первых построений. Замысел ее основан на следующем соображении. Пусть $x^2 - dy^2 = 1$ — уравнение Пелля ($d \in Z^+$ — целое число, не являющееся полным квадратом). Его решения $\langle x, y \rangle \in (Z^+)^2$ образуют полугруппу относительно закона композиции

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_3 + y_3\sqrt{d}.$$

Эта полугруппа циклична. Иными словами, пусть $\langle x_1, y_1\rangle$ — решение с наименьшей первой координатой. Тогда любое другое решение имеет вид $\langle x_n, y_n\rangle$, где $n \in Z^+$, и

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

Число n назовем *номером* решения $\langle x_n, y_n\rangle$.

Координаты x_n, y_n растут с n экспоненциально, так что множество решений уравнения Пелля, а также его проекции на x- и y-оси являются диофантовыми множествами логарифмической плотности. Это — еще не то, что нужно: основная трудность состоит в том, чтобы включить номер решения n в число координат диофантова множества — только тогда мы получим возможность применить дальнейшие соображения. Это и будет сделано ниже.

5.2. Обозначения. Рассмотрим уравнение Пелля с переменным d. Его первое решение меняется в зависимости от d, вообще говоря, очень неконтролируемым образом, поэтому удобно отобрать лишь часть d, для которых первое решение иметь простой специальный вид $\langle a, 1\rangle$, $a \in Z^+$. Очевидно, тогда $d = a^2 - 1$.

Уравнение $x^2 - (a^2 - 1)y^2 = 1$ будем называть *a-уравнением*. Определим две последовательности чисел $x_n(a)$, $y_n(a)$ как координаты его n-решения:

$$x_n(a) + y_n(a)\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n.$$

Формальное определение $x_n(a)$ и $y_n(a)$ как многочленов от a легко дать индукцией по n. Тогда выражения $x_n(a)$, $y_n(a)$ будут иметь смысл для всех $n \in Z$ и $a \in C$. В частности,

$$x_n(1) = 1, \quad y_n(1) = n;$$

при этом все приводимые ниже формулы останутся справедливыми. Основным результатом этого параграфа является

5.3. Предложение. *Множество в $\langle y, n, a\rangle$-пространстве*

$$E: y = y_n(a), \quad a > 1$$

является диофантовым.

В доказательстве используются элементарные теоретико-числовые свойства последовательностей $x_n(a)$, $y_n(a)$.

Их проверки в основном отнесены в конец параграфа (см. п. 5.8).

Идея диофантового восстановления n по $\langle y, a\rangle$ состоит в замечании, что

$y_n(a) \equiv n \bmod (a - 1)$ (лемма 5.4).

Это однозначно определяет n, если только $n < a - 1$. Чтобы перейти к общему случаю, вводится вспомогательное A — уравнение с большим A, и его n-е решение, которое следует (с помощью y) определить так, чтобы использовать n лишь в диофантовом контексте.

Формально диофантовость E устанавливается по схеме, описанной в п. 4.2. Кроме основных переменных y, n, a, вводятся шесть вспомогательных: x; x', y'; A; x_1, y_1. Положим далее

$E_1 : y \geqslant n,\ a > 1;$

$E_2 : x^2 - (a^2 - 1)y^2 = 1;$

$E_3 : y' \equiv 0 \bmod 2x^2y^2;$

$E_4 : x'^2 - (a^2 - 1)y'^2 = 1;$

$E_5 : A = a + x'^2(x'^2 - a);$

$E_6 : x_1^2 - (A^2 - 1)\, y_1^2 = 1;$

$E_7 : y_1 - y \equiv 0 \bmod x'^2;$

$E_8 : y_1 \equiv n \bmod 2y.$

Пусть $E' = \bigcap_{i=1}^{8} E_i$. Покажем, что $\operatorname{pr} E' = E$.

Включение $E \subseteq \operatorname{pr} E'$. Даны $\langle y, n, a\rangle \in E$; нужно подобрать значения остальных переменных так, чтобы удовлетворить $E_1, \ldots, E_8$. Как и выше, мы не будем вводить для них специальных символов; после выбора, скажем, значения x буква x далее становится именем этого значения.

E_1 удовлетворяется автоматически: $y_n(a) \geqslant n$ для всех $a \geqslant 1$, $n \geqslant 1$ (индукция по n). Найдем единственное x из E_2: $x = x_n(a)$. В качестве $\left\langle x', \dfrac{y'}{2x^2y^2}\right\rangle$ возьмем любое решение уравнения Пелля $X^2 - (a^2 - 1)(2x^2y^2)^2 Y^2 = 1$.

Это даст $E_4 \cdot A$ однозначно находится из E_5. В качестве $\langle x_1, y_1\rangle$ возьмем n-е решение A-уравнения. Все выборы произведены. Для проверки E_7 и E_8 нам понадобятся две леммы:

5.4. Лемма. $y_k(a) \equiv k \bmod (a - 1)$.

5.5. Лемма. *Если* $a \equiv b \bmod c$, *то* $y_n(a) \equiv y_n(b) \bmod c$.

Доказательства их см. в п. 5.8.

Используются они так. Из E_5 находим

$$A = a + (1 + ay'^2)(1 + ay'^2 - a) \equiv 1 \bmod 2y$$

с учетом E_3. Лемма 5.4 тогда дает

$$y_1 = y_n(A) \equiv n \bmod 2y:$$

это E_8.

Лемма 5.5 дает $y_n(A) \equiv y_n(a) \bmod x'^2$ (с учетом E_5): это E_7.

Включение $\operatorname{pr} E \subseteq E$. Из соотношений $E_1, \ldots, E_8$ мы должны только вывести, что n есть номер решения $\langle x, y\rangle$. Заметим, что n участвует лишь в E_8.

Временно обозначим через N, N', N_1 номера решений $<x, y>$, $<x', y'>$, $<x_1, y_1>$ соответственно. Мы докажем, что

$n \equiv N$ или $n \equiv -N \bmod 2y$.

Так как, кроме того, $y \geqslant n$ (E_1) и $y \geqslant N$ (определение N), это дает $N = n$, что и требуется. Номер N_1 будет «посредником» между n и N.

Прежде всего из E_5 находим, как выше,

$A \equiv 1 \bmod 2y$

и затем из определения N_1 и леммы 5.4

$y_1 \equiv N_1 \bmod 2y$.

Но по E_8 $y_1 \equiv n \bmod 2y$; поэтому

$N_1 \equiv n \bmod 2y$.

Далее, из E_5, $A \equiv a \bmod x'^2$ и затем

$y_1 = y_{N_1}(A) \equiv y_{N_1}(a) \bmod x'^2$

по лемме 5.5. В силу E_7

$y = y_N(a) \equiv y_1 \bmod x'^2$,

поэтому

$y_N(a) \equiv y_{N_1}(a) \bmod x'^2$.

Для дальнейшего нам понадобятся еще две леммы, которые мы докажем в п. 5.8.

5.6. **Лемма.** *Если* $y_i(a) \equiv y_j(a) \bmod x_n(a)$, $a > 1$, *то* $i \equiv j$ *или* $i \equiv -j \bmod 2n$.

5.7. **Лемма.** *Если* $y_i(a)^2 / y_j(a)$, *то* $y_i(a) / j$.

Лемма 5.6, примененная к N, N_1, N' вместо i, j, n, с учетом последнего доказанного сравнения дает

$N \equiv \pm N_1 \bmod 2N'$.

Лемма 5.7, примененная к N, N' вместо i, j, с учетом E_3 дает y / N'. Поэтому

$N \equiv \pm N_1 \bmod 2y$.

Так как мы уже установили, что $N_1 \equiv n \bmod 2y$, это заканчивает доказательство.

5.8. Доказательство леммы. Будем писать $x_n y_n$ вместо $x_n(a)$, $y_n(a)$. Из формулы

$$x_{nk} + y_{nk}\sqrt{a^2-1} = (x_n + y_n\sqrt{a^2-1})$$

находим

$$y_{nk} = \sum_{\substack{j \leqslant k \\ j \equiv 1\,(2)}} \binom{k}{j} x_n^{k-j} y_n^j (a^2-1)^{(j-1)/2}.$$

В частности,

$$y_{nk} \equiv k x_n^{k-1} y_n \bmod (a^2-1),$$

что дает лемму 5.4 при $n = 1$. Кроме того,

$$y_{nk} \equiv k x_n^{k-1} y_n \bmod y_n^3.$$

Заменив здесь nk, k, n на n, n/k, k, получим

$$y_n \equiv \frac{n}{x} x_k^{\frac{n}{k}-1} y_k \bmod y_k^3.$$

Так как $(x_k, y_k) = 1$, находим отсюда

$$y_n \equiv 0 \bmod y_k^2 \Rightarrow \frac{n}{k} \equiv 0 \bmod y_k \Rightarrow n \equiv 0 \bmod y_k,$$

что дает лемму 5.7.

Выражение $y_n(a)$ в виде универсального многочлена от a, коэффициенты которого целы и зависят (вместе со степенью) лишь от n, немедленно дает лемму 5.5.

Остается доказать лемму 5.6.

Прежде всего из равенства

$$x_{n \pm m} + \sqrt{a^2-1}\, y_{n \pm m} = (x_n + \sqrt{a^2-1}\, y_n)(x_m \pm \sqrt{a^2-1}\, y_m)$$

находим

$$x_{n \pm m} = x_n x_m \pm (a^2-1) y_n y_m,$$

$$y_{n \pm m} = \pm x_n y_m + x_m y_n.$$

Отсюда

$$y_{2n \pm m} = y_{n + (n \pm m)} \equiv x_{n \pm m} y_n \bmod x_n \equiv \pm (a^2-1) y_n^2 y_m \bmod x_n \equiv$$
$$\equiv \mp y_m \bmod x_n$$

и аналогично

$$y_{4n \pm m} = y_{2n + (2n \pm m)} \equiv -y_{2n \pm m} \bmod x_n \equiv y_{\pm m} \bmod x_n.$$

Это означает, что как функция от k класс $y_k \bmod x_n$ имеет период $4n$; внутри же периода $[1, 4n]$ поведение определяется его первой четвертью $[1, n]$:

$$y_{2n \pm m} \equiv \mp y_m, \; y_{\pm m} \equiv \pm y_m \quad \text{при} \quad 1 \leqslant m \leqslant n.$$

Теперь при $a \geqslant 3$ лемма 5.6 следует из этих факторов и из того, что $y_m < 0{,}5x_n$ при $1 \leqslant m \leqslant n$. Действительно,

$$4y_m^2 < (a^2-1)\,y_n^2 + 1 = x_n^2.$$

При $a = 2$ имеем $y_m < 0{,}5x_n$ только для $m \leqslant n-1$, но и этого достаточно для доказательства леммы.

6. ГРАФИК ЭКСПОНЕНТЫ ДИОФАНТОВ

6.1. Предложение. *Множество*

$$E : y = a^n$$

в $\langle y, a, n\rangle$ *— пространстве диофантово.*

Доказательство. Достаточно проверить диофантовость

$$E_0 = E \cap \{a \mid a > 1\}.$$

При $a > 1$ индукцией по n легко получаем

$$(2a-1)^n \leqslant y_{n+1}(a) \leqslant (2a)^n$$

в обозначениях § 5. Отсюда для любого $N \geqslant 1$ имеем

$$a^n\left(1-\frac{1}{2Na}\right)^n = \frac{(2Na-1)^n}{(2N)^n} \leqslant \frac{y_{n+1}(Na)}{y_{n+1}(N)} \leqslant \frac{(2Na)^n}{(2N-1)^n} = a^n\left(1-\frac{1}{2N}\right)^{-n}.$$

Значит, если выбрать N столь большим, чтобы одновременно

$$\left(1-\frac{1}{2N}\right)^{-n} - 1 < \frac{1}{a^n},$$

$$1-\left(1-\frac{1}{2Na}\right)^n < \frac{1}{a^n},$$

то получим $a^n = [y_{n+1}(Na)/y_{n+1}(N)]$ (квадратные скобки здесь и ниже означают целую часть числа). Таким образом, E_0 есть проекция множества E_1:

$$a > 1;$$
$$0 \leqslant y_{n+1}(N)\,y - y_{n+1}(Na) < y_{n+1}(y),$$
$$N > ?,$$

где вместо ? нужно поставить подходящую нижнюю оценку N, в то же время позаботившись о диофантовости этого последнего соотношения. Элементарные оценки показывают, что достаточно положить $N > 4n(y+1)$.

Диофантовость E_1 можно получить тогда из результатов § 5 с помощью введения тривиальных вспомогательных соотношений

$$y' = y_{n+1}(N) \text{ и } y'' = y_{n+1}(Na).$$

7. ГРАФИКИ ФАКТОРИАЛА И БИНОМИАЛЬНЫХ КОЭФФИЦИЕНТОВ ДИОФАНТОВЫ

В этом параграфе проведена последняя серия рассуждений.

7.1. Предложение. *Множество*

$$E : r = \binom{n}{k}, \quad n \geqslant k,$$

в $<r, k, n>$*-пространстве диофантово.*

Здесь по определению $\left(\frac{n}{k}\right) = \frac{n(n-1)\ \ldots\ (n-k+1)}{k!}$. Для доказательства нужна следующая лемма.

7.2. Лемма. *Если* $u > n^k$, *то* $\binom{n}{k}$ = *остаток от деления* $[(u+1)^n/u^k]$ *на* u.

Доказательство. Имеем

$$(u+1)^n/u^k = \sum_{i=k+1}^{n} \binom{n}{i} u^{i-k} + \binom{n}{k} + \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k}.$$

Первая сумма делится на u, а последняя меньше единицы при $u > n^k$.

7.3. Доказательство предложения 7.1. Введем вспомогательные переменные u, v и соотношения

$E_1 : u > n^k$;

$E_2 : v = [(u+1)^n/u^k]$;

$E_3 : r \equiv v \bmod u$;

$E_4 : r < u$;

$E_5 : n \geqslant k$.

Из леммы немедленно следует, что $E = \operatorname{pr} \bigcap_{i=1}^{5} E_i$. Диофантовость E_1 следует из диофантовости экспоненты; диофантовость E_3, E_4 и E_5 очевидна. Диофантовость E_2 становится ясной, если представить E_2 в виде

$$(u+1)^n \leqslant u^k v < (u+1)^n + u^k$$

и воспользоваться снова диофантовостью экспоненты.

Предложение доказано.

7.4. Предложение. *Множество* $E : m = k!$ *диофантово.*

7.5. Лемма. *Если* $k > 0$ *и* $n > (2k)^{k+1}$, *то* $k! = \left[\frac{n^k}{\binom{n}{k}}\right]$.

(Доказательство получается легкими оценками.)

Доказательство предложения. Вспомогательная переменная n; соотношения

$E_1 : n > (2k)^{k+1}$;

$$E_2 : m = \left[\frac{n^k}{\binom{n}{k}}\right].$$

Дальнейшее очевидно (используются доказанные ранее диофантовость экспоненты и биномиальных коэффициентов).

7.6. **Предложение.** *Множество*

$$E : \frac{x}{y} = \binom{p/q}{k}, \quad p > qk,$$

в пространстве $\langle x, y, p, q, k\rangle$ *— диофантово.*

Доказательство является некоторым усложнением рассуждений из п. 7.2, 7.3.

7.7. **Лемма.** *Пусть* $a > 0$ *— такое целое число, что* $a \equiv 0\ (q^k k!)$ *и* $a > 2^{p-1} p^{k+1}$.

Тогда

$$\binom{p/q}{k} = a^{-1}\left[a^{2k+1}\left(1 + a^{-2}\right)^{p/q}\right] - a\left[a^{2k-1}\left(1 + a^{-2}\right)^{p/q}\right].$$

Доказательство получается разложением $(1 + a^{-2})^{p/q}$ в биномиальный ряд Тейлора. Неравенство позволяет при переходе к целой части отбросить в первом слагаемом все члены, начиная с $(k + 1)$-го, а во втором — начиная с k-го. Сравнение $a \equiv 0\ (q^k k!)$ обеспечивает целость неполных сумм.

7.8. Доказательство предложения. Вспомогательные переменные a, u_1, u_2, v. Соотношения

$E_1 : a \equiv 0 \bmod q^k k!$;

$E_2 : a > 2^{p-1} p^{k+1}$;

$E_3 : u_1/u_2 = a^{-1}\left[a^{2k+1}\left(1 + a^{-2}\right)^{p/q}\right]$;

$E_4 : v = a\left[a^{2k-1}\left(1 + a^{-2}\right)^{p/q}\right]$.

Условие $E = \mathrm{pr} \bigcap_{i=1}^{4} E_i$ следует из леммы. Диофантовость E_1 и E_2 непосредственно следует из диофантовости экспоненты и факториала. Диофантовость E_3 и E_4 устанавливается, как в конце п. 7.3; нужно не только избавиться от знаменателя, но еще и возвести неравенства в q-ю степень.

Это завершает доказательство теоремы 1.2 о совпадении классов перечислимых и диофантовых множеств.

8. ДОПОЛНЕНИЯ

После того как был доказан принципиальный результат о диофантовости перечислимых множеств, появилось много работ, усовершенствующих доказательства и дающих более экономные диофантовы представления. В этом параграфе мы приведем несколько результатов такого рода, отсылая за доказательствами к оригинальным статьям.

8.1. Универсальный многочлен. Согласно теореме 1.2 всякое перечислимое подмножество Z^+ можно представить в виде проекции подмножества вида $P = 0$ в $(Z^+)^{n+1}$, где P — многочлен с целыми коэффициентами. В § 1 следующей главы мы несколько усилим этот результат, построив версальное семейство перечислимых подмножеств в Z^+ и представив его в виде проекции подмножества вида $U = 0$ в $(Z^+)^{n+2}$ на $Z^+ \times Z^+$, где U — многочлен с целыми коэффициентами.

Назовем такой многочлен U универсальным. В его записи заключена программа для порождения всех перечислимых подмножеств Z^+; важно знать, насколько сложно устроен U. Эту сложность можно измерять разными способами. Существенно было бы узнать, каково наименьшее возможное значение числа n, т. е. коразмерности проекции. Ю. В. Матиясевич показал, что можно построить универсальный многочлен U с $n = 9$, но у него очень большая степень — по оценке Дж. Джоунза, она имеет порядок $1{,}6 \cdot 10^{45}$. С другой стороны, можно построить универсальный многочлен степени всего 4, но с $n = 58$. Другие возможные значения степени и коразмерности суть: (38,8); (32,12); (24,36); (19,2668). Еще одна естественная мера сложности U — количество Ω сложений и умножений, необходимое, чтобы вычислить любое его значение. Дж. Джоунз доказал, что можно построить U, для которого $\Omega = 100$.

Приведем теперь два конкретных диофантовых представления.

8.2. Простые числа. Множество простых чисел совпадает с множеством положительных значений, которые принимает в целых точках многочлен степени 25 от 26 переменных (все буквы английского алфавита!):

$$(k+2)\{1 - [wz + h + j - q]^2 - [(gk + 2g + k + 1)(h + j) + h - z]^2 - [2n + p + q + z - e]^2 - [16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2 - [e^3(e+2)(a+1)^2 + 1 - o^2]^2 - [(a^2-1)y^2 + 1 - x^2]^2 - [16r^2y^4(a^2-1) + 1 - u^2]^2 - [((a + u^2(u^2-a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 - [n + l + v - y]^2 - [(a^2-1)l^2 + 1 - m^2]^2 - [ai + k + 1 - l - i]^2 - [p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 - [q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 - [z + pl(a - p) + t(2ap - p^2 - 1) - pm]^2\}.$$

Этот многочлен был предложен в работе Дж. Джоунза, Д. Сато, Х. Вада и Д. Вайэнса [22].

8.3. **Числа Фибоначчи.** Они образуют последовательность 1, 1, 2, 3, 5, 8, ...; $u_{n+2} = u_{n+1} + u_n$
Дж. Джоунз нашел, что в отличие от простых чисел эта последовательность совпадает с множеством положительных значений совсем простого многочлена пятой степени от двух переменных:
$2a^4b + a^3b^2 - 2a^2b^3 - a^5 - ab^4 + 2a$.

Глава III

СЛОЖНОСТЬ И СЛУЧАЙНОСТЬ

1. ВЕРСАЛЬНЫЕ СЕМЕЙСТВА

Версальные семейства были определены и впервые использованы в п. 5.7 гл. I; цель этого параграфа — доказать их существование с помощью теоремы 1.2 гл. II о диофантовости перечислимых множеств.

1.1. Теорема. *Для любого $m \geqslant 0$ версальные перечислимые семейства m-множеств и m-функций с базой Z^+ существуют и могут быть эффективно построены.*

Следствие. *Существуют перечислимые, но не разрешимые множества.*

(Введено в п. 5.8 гл. I; использовано в п. 1.3 гл. II.)

Доказательство. Мы разобъем его на несколько этапов. Напомним, что $\tau^{(2)} : (Z^+)^2 \to Z^+$ — примитивно-рекурсивный изоморфизм, построенный в § 4 гл. I, $\langle t_1^{(2)}, t_2^{(2)} \rangle$ — обратный ему. Будем писать t_1, t_2 для краткости.

а) *Версальное семейство многочленов из* $Z^+[x_1, x_2, x_3, \ldots]$. Определим многочлены $f[l] \in Z^+[x_1, x_2, x_3, \ldots]$ рекурсией по $l \in Z^+$, $l \geqslant 4$:

$$f[1] = f[2] = f[3] = 1,$$
$$f[4k] = k;$$
$$f[4k+1] = x_k;$$
$$f[4k+2] = f[t_1(k)] + f[t_2(k)];$$
$$f[4k+3] = f[t_1(k)] f[t_2(k)].$$

Определение корректно, ибо $t_1(k), t_2(k) < 4k + 2$. Образ отображения $k \to f[k]$ совпадает со всем кольцом, ибо он содержит Z^+ (на местах $4k$), все x_k (на местах $4k + 1$) и вместе с двумя многочленами $f[k_1]$ и $f[k_2]$ их сумму (на месте $4\tau^{(2)}(k_1, k_2) + 2$) и произведение (на месте $4\tau^{(2)}(k_1, k_2) + 3$).

б) *Конструкция версального 1-семейства над* Z^+. Положим E_k = проекция на x_1-координату 0-уровня многочлена

$$f\,[t_1\,(k)] - f\,[t_2\,(k)].$$

Так как все элементы $Z\,[x_1, x_2, x_3, \ldots]$ представимы в виде таких разностей, ясно, что семейство $\{E_k\}$ содержит все перечислимые множества.

в) $\{E_k\}$ *перечислимо.* Мы должны установить перечислимость тотального пространства

$$E = \{\langle i, j\rangle \mid i \in E_j\} \subset Z^+ \times Z^+.$$

Запишем условие $\langle i, j\rangle \in E$ в виде логической формулы типа α_1 (см. Д и НД), где все кванторы относятся к переменным, принимающим значения в Z^+. Учтем, что

$$f\,[t_1\,(j)] - f\,[t_2\,(j)] \in Z\,[x_1, \ldots, x_j].$$

Имеем

$$\langle i, j\rangle \in E \Leftrightarrow i \in E_j \Leftrightarrow \exists x_1 \ldots \exists x_j\,(x_1 = i \wedge f\,[t_1\,(j)] =$$
$$= f\,(t_2\,(j)]) \Leftrightarrow \exists t\,((\exists x_1 \ldots \exists x_j \forall k \leqslant j\,(f\,[k] = \mathrm{Gd}\,(k, t))) \wedge \mathrm{Gd}\,(1, t) =$$
$$= \mathrm{Gd}\,(2, t) = \mathrm{Gd}\,(3, t) = 0 \wedge \mathrm{Gd}\,(5, t) = i \wedge \mathrm{Gd}\,(t_1\,(j), t) = \mathrm{Gd}\,(t_2\,(j), t)),$$

где $\mathrm{Gd}\,(k, t)$ — функция Геделя (§ 4 гл. I).

Далее, по определению $f\,[k]$

$$\exists x_1 \ldots \exists x_j \forall k \leqslant j\,(f\,[k] = \mathrm{Gd}\,(k, t)) \Leftrightarrow \forall k \leqslant j\,((k \leqslant 3 \wedge \mathrm{Gd}\,(k, t) = 0) \vee$$
$$\vee \exists l\,((k = 4l \wedge \mathrm{Gd}\,(k, t) = l) \vee (k = 4l + 2 \wedge \mathrm{Gd}\,(k, t) =$$
$$= \mathrm{Gd}\,(t_1\,(l), t) + \mathrm{Gd}\,(t_2\,(l), t)) \vee (k = 4l + 3 \wedge \mathrm{Gd}\,(k, t) =$$
$$= \mathrm{Gd}\,(t_1\,(l), t)\,\mathrm{Gd}\,(t_2\,(l), t)))).$$

Здесь формула, следующая за $\exists l$, определяет разрешимое множество в $\langle k, t, l\rangle$-пространстве. Квантор $\exists l$ превращает его в перечислимое, проектируя на $\langle k, t\rangle$-координаты, а ограниченный квантор $\forall k \leqslant j$ не нарушает перечислимости (см. § 2 гл. II). Переходя к формуле, определяющей E, мы обнаруживаем, что нужно пересечь построенное множество еще с тремя разрешимымы и спроектировать вдоль t-оси, так что результат снова перечислим.

г) *Конструкция версального* m-*семейства над* Z^+. Случай $m = 0$ тривиален; $m = 1$ уже разобран; $m \geqslant 2$ сводится к $m = 1$ с помощью изоморфизма

$$\tau^{(m)} : (Z^+)^m \simeq Z^+.$$

Пусть $E_k = E_k^{(1)}$ — версальное 1-семейство; положим $E_k^{(m)} = (\tau^m)^{-1}\,(E^1)$.

Перечислимость $\{E^{(m)}_k\}$ следует из того, что

$$E^{(m)} = \{\langle x, k\rangle \mid x \in E^{(m)}_k\} = \{\langle (\tau^{(m)})^{-1}(x), k\rangle \mid x \in E^{(1)}_k\} = (\tau^{(m)}, \mathrm{pr}^1_1)^{-1} E^{(1)}.$$

д) *Конструкция версального семейства 1-функций.* Рассмотрим версальное семейство 2-множеств $\{E^{(2)}_k\}$ с остальным пространством $E^{(2)}$:

$$E^{(2)} = \{\langle x, y, k\rangle \mid \langle x, y\rangle \in E^{(2)}_k\} \subset (Z^+)^3.$$

Пусть $g(x, y, k, z)$ — примитивно рекурсивная функция, проекция 1-уровня которой на $\langle x, y, k\rangle$-пространство совпадает с $E^{(2)}$. Положим

$$f(x, k) = t^{(2)}_1(\min\{u \mid g(x, t^{(2)}_1(u), k, t^{(2)}_2(u)) = 1.$$

Утверждается что $\{f_k(x) = f(x, k)\}$ есть версальное семейство 1-функций. Тотальная функция, очевидно, рекурсивна. Нужно проверить лишь, что всякая частично рекурсивная 1-функция f встречается в семействе.

Пусть Γ_f — ее график и $\Gamma_f = E^{(2)}_{k_0}$, $k_0 \in Z^+$. Покажем, что тогда $f = f_{k_0}$. Действительно,

$$\langle x, f(x)\rangle \in \Gamma_f = E^{(2)}_{k_0} \Leftrightarrow \langle x, f(x), k_0\rangle \in E^{(2)} \Leftrightarrow \exists z \in Z^+,$$

$$g(x, f(x), k_0, z) = 1.$$

Выберем среди подходящих $z \in Z^+$ такое, чтобы число u, найденное из условия

$$\langle f(x), z\rangle = \langle t^{(2)}_1(u), t^{(2)}_2(u)\rangle,$$

было наименьшим. Для этого u имеем

$$f_{k_0}(x) = t^{(2)}_1(u) = f(x),$$

что доказывает требуемое.

е) *Конструкция версального семейства m-функций.* Случай $m = 0$ тривиален; если $\{f^{(1)}_k\}$ — версальное семейство 1-функций, то полагая при $m \geqslant 2$

$$f^{(m)}_k(x_1, \ldots, x_m) = f^{(1)}_k(\tau^{(m)}(x_1, \ldots, x_m)),$$

получаем версальное семейство m-функций.

Теорема доказана.

1.2. Выбор версальных семейств весьма не однозначен. Универсальных семейств, содержащих каждую функцию (соответственно каждое множество) точно по одному разу, при $m \geqslant 1$ не существует. Тем не менее есть важные способы извлекать инвариантную информацию из сведений о положении функции (множества) в версальном семействе. Этому посвящен следующий параграф.

2.1. Пусть $u = \{u_k\}$ — перечислимое семейство m-функций над Z^τ, f — некоторая частично рекурсивная m-функция.

Сложность f относительно семейства u определяется так:

$$C_u(f) = \begin{cases} \min\{k \mid u_k = f\}, & \text{если такое } k \text{ существует;} \\ \infty & \text{в противном случае.} \end{cases}$$

Перечислимое семейство u называется (асимптотически) оптимальным, если для любого другого перечислимого семейства v существует такая константа $c_{u,v} > 0$, что для всякой частично рекурсивной m-функции f имеем

$$C_u(f) \leqslant c_{u,v} C_v(f).$$

Взяв здесь в качестве v любое версальное семейство, находим, что оптимальное семейство должно быть версальным (бесконечных значений $C_u(f)$ не принимает).

2.2. Теорема Колмогорова. а) *Для любого $m \geqslant 0$ оптимальные семейства существуют и могут быть эффективно построены.*

б) *Если u, v — оптимальные семейства m-функций, то для любой m-функции f*

$$c_{vu}^{-1} \leqslant \frac{C_u(f)}{C_v(f)} \leqslant c_{uv}.$$

2.3. Замечания. а) С мерой сложности $C_u(f)$ связаны следующие интуитивные представления. Чтобы определить любое перечислимое семейство u, достаточно задать некоторую конечную информацию: скажем, программу, полувычисляющую тотальную функцию u.

Чтобы определить конкретную функцию f, встречающуюся в семействе u, достаточно поэтому задать не больше $\log_2 C_u(f) + \text{const}$ бит информации: к программе для u следует приписать номер f.

б) Оптимальность семейства означает, что оно годится для вычисления любой m-функции и что проигрыш в длинах вычисляющих программ по сравнению с любым другим семейством ограничен константой, не зависящей от функции.

в) Наконец, неравенство б), тривиально следующее из определения оптимальности, показывает, что логарифмическая мера сложности Колмогорова

$$K_u(f) = \lfloor \log_2 C_u(f) \rfloor + 1$$

с точностью до ограниченного по модулю слагаемого не зависит от выбора оптимального семейства u и, значит, является асимптотически инвариантной характеристикой f.

2.4. Доказательство теоремы 2.2. а) Выберем рекурсивное вложение θ: $Z^+ \times Z^+ \to Z^+$ с рекурсивной обратной функцией; удовлетворяющей условию линейности роста по одному аргументу: $\theta(k, j) \leqslant k\varphi(j)$ для всех $k, j \in Z^+$ и подходящей φ: $Z^+ \to Z^+$. Например, можно положить $\theta_1(k, j) = (2k-1)2^j$ с $\varphi_1(j) = 2^{j+1}$ или, по Колмогорову,

$$\theta_2(\overline{k_1 k_2 \ldots k_r}, \overline{j_1 \ldots j_s}) = \overline{j_1 j_1 \ldots j_s j_s 0\, 1\, k_1 \ldots k_r},$$

где $k_\alpha, j_\beta \in \{0, 1\}$, а черта подразумевает двоичное разложение. Здесь $\varphi_2(j) < \text{const}\, j_2$, так что эта функция экономнее по росту. Ср. также с п. 2.8 ниже.

б) Пусть U — любое версальное семейство $(m+1)$-функций. Определим семейство m-функций u, положив

$$u(x_1, \ldots, x_m, k) = U(x_1, \ldots, x_m, \theta^{-1}(k)).$$

Покажем, что оно оптимально, со следующей оценкой констант:

$$c_{uv} \leqslant \varphi(C_u(v)).$$

В самом деле, пусть f — рекурсивная m-функция. Достаточно разобрать случай, когда она встречается в семействе v. Тогда

$$f(x_1, \ldots, x_m) = v(x_1, \ldots, x_m; C_v(f)) = U(x_1, \ldots, x_m, C_v(f); C_u(v)) = u(x_1, \ldots, x_m, \theta(C_v(f), C_u(v)),$$ откуда

$$C_u(f) \leqslant \theta(C_v(f), C_u(v)) \leqslant C_v(f)\varphi(C_u(v)).$$ Теорема доказана.

2.5. Пример. O-функцию f можно отождествить с ее единственным значением, т. е. с положительным целым числом n. Таким образом, теорема 2.2 определяет почти инвариантную сложность целых чисел $C_u(n)$. Имеем

а) $C_u(n) \leqslant \text{const}\ n$ для всех n, ибо в простейшем версальном семействе $u_n(\cdot) = n$ функция «n» появляется на n-м месте.

б) $C(n) \sim \min\{2^{j-1}(2k-1) \mid n$ есть k-е значение j-й функции в каком-нибудь версальном семействе 1-функции$\}$.

(Здесь и ниже мы будем писать $f \sim g$, если f, g имеют общую область определения, $f \leqslant \text{const}_1 g$ и $g \leqslant \text{const}_2 f$ для подходящих констант. В соотношениях типа $C_u(f_k) \sim g(k)$ можно опускать упоминание оптимального семейства u, считая, что u произвольно, но фиксировано.)

Из б) видно, что при $n \to \infty$ сложность чисел p_n (n-е простое число), n^2 или $n^{n^{\cdot^{\cdot^{\cdot^n}}}}$ (n раз) асимптотически не больше const n, ибо все это — n-е значения фиксированной рекурсивной функции. Ниже в п. 2.7б эта оценка будет уменьшена до const $C(n)$.

Колмогоров рассматривал вместо целых чисел конечные двоичные последовательности и построил вместе с сотрудниками теорию, показывающую, что максимально сложные двоичные последовательности

ведут себя подобно случайным. См. ее обзор в статье А. К. Звонкина и Л. А. Левина в УМН, 1970 т. XXV, вып. 6, с. 85—127, содержащей большую библиографию. В § 3 изложены некоторые результаты из этой статьи

2.6. Предложение. а) *Пусть*

$$F = f_0(f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m), x_{n+1}, \ldots, x_p),$$

где f_i *— рекурсивные функции. Тогда*

$$C(F) \leqslant \text{const} \prod_{i=1}^{n} C(f_i) \left(\log \prod_{i=1}^{n} C(f_i) \right)^{n-1}.$$

если f_0 *фиксирована, а* f_i *пробегает все возможные т-функции Здесь* const *зависит от* f_0 *и семейства, относительно которых вычисляется сложность, но не от* $f_1, \ldots, f_n$.

б) *Если позволить менять также* f_0, *справа следует заменить* $\prod_{i=1}^{n}$ *на* $\prod_{i=0}^{n}$ *и* $\log^{n-1}$ *на* $\log^n$.

2.7. Частные случаи. а) Полагая $f_0 = \text{sum}_2$ или prod_2 получаем, например

$$C(f_1 + f_2),\ C(f_1, f_2) \leqslant \text{const}\ C(f_1)C(f_2) \log (C(f_1)C(f_2)).$$

б) Полагая $n = 1$, $m = 0$, получаем для любого перечислимого семейства $\{f_k\}$

$$C(f(k, x_1, \ldots, x_p)) \leqslant \text{const}\ C(k).$$

2.8. Доказательство предложения 2.6. Прежде всего для каждого $n \geqslant 1$ определим следующую рекурсивную биекцию с рекурсивной обратной:

$$0^{(n)}(k_1, \ldots, k_n) = \begin{cases} \text{номер } n\text{-ки } \langle k_1, \ldots, k_n \rangle \text{ при упорядочении их в по} \\ \text{рядке возрастания } \prod_{i=1}^{n} k_i, \text{ а при данном } \prod_{i=1}^{n} k_i - \\ \text{— в словарном порядке.} \end{cases}$$

Нетрудно убедиться (индукция по n), что

$$\Theta^{(n)}(k_1, \ldots, k_n) \leqslant \text{const} \prod_{i=1}^{n} k_i \left(\log \prod_{i=1}^{n} k_i \right)^{n-1}.$$

Определим фукцию $\Xi : (Z^+)^{n+1} \to Z^+$:

$$\Xi(l_1, \ldots, l_{n+1}) = \theta(\theta^{(n)}(l_1, \ldots, l_n), l_{n+1}),$$

где Θ выбрана, как в п. 2.4.

Далее рассмотрим два оптимальных семейства: p-функций $v(x_1, \ldots, x_p, l)$ и m-функций $u(x_1, \ldots, x_m, k)$. Наконец, построим по ним семейства

$$W(x_1, \ldots, x_p; k_1, \ldots, k_n, l) = v(u(x_1, \ldots, x_m, k_1), \ldots, u(x_1, \ldots, x_m, k_n), x_{n+1}, \ldots, x_p, l),$$
$$w(x_1, \ldots, x_p, k)) = W(x_1, \ldots, x_p, \Xi^{-1}(k)).$$

Функция F встречается в семействе w на месте

$$\Theta(\Theta^{(n)}(C_u(f_1), \ldots, C_u(f_n)), C_v(f_0)),$$

и оценка $\Theta(k, j) \leqslant k\,\varphi(j)$ вместе с оценкой для $\Theta^{(n)}$ дают утверждение а) теоремы.

Утверждение б) получится аналогично, если в определении w заменить Ξ на $\Theta^{(n+1)}$.

2.9. Замечание. Функция $\theta^{(n)}$ приводит к самой экономной оценке $C(F)$, симметричной относительно $C(f_1), \ldots, C(f_n)$. В конкретных задачах может оказаться полезным улучшить оценку, скажем, по некоторым из $C(f_i)$ за счет ее ухудшения по остальным: для этого нужно соответствующим образом изменить $\Theta^{(n)}$. Например, Θ Колмогорова дает

$$C(f_1 + f_2) \leqslant \text{const}\, C(f_1)C(f_2)^2,$$

что при очень слабо растущей $C(f_2)$ (по сравнению с $C(f_1)$) выгоднее, чем $\text{const}\, C(f_1)C(f_2) \log(C_2(f_1)C(f_2))$.

2.10. Теорема. Функция $C(f)$ невычислима.

Точнее, пусть $g(k)$ — любая неограниченная частично рекурсивная функция, $\{f_k\}$ — любое перечислимое семейство. Тогда неверно, что $C(f_k) \mid_{D(g)} \sim g(k)$.

Таким образом, $C(f_k)$ может быть вычислимой, даже с точностью до $\sim$, только на таком множестве индексов k, где среди функций f_k есть лишь конечное число разных — иначе $\mathcal{C}(f_k)$ на этом множестве не ограничена.

Доказательство. Предположим, что $C(f_k) \mid_{D(g)} \sim g(k)$.

Покажем, что существует общерекурсивная функция $h: Z^+ \to Z^+$, образ которой принадлежит $D(g)$ и такая, что $g \circ h$ монотонно возрастает. Противоречие получается отсюда так: для всех k имеем в силу 2.7б)

$$C(f_{h(k)}) \leqslant \text{const}\, C(k),$$

в силу предположения и возрастания $g \cdot h$

$$C(f_{h(k)}) \geqslant \text{const}\, g(h(k)) \geqslant \text{const}\, k.$$

Эти два неравенства несовместимы, потому что $\lim \frac{C(k)}{k} = 0$, например $\frac{C(k^2)}{k^2} \leqslant \frac{\text{const}}{k}$.

Остается построить h. Выберем общерекурсивную биекцию $h_1 : Z^+ \to D(g)$ (предложение 5.6 гл. I), положим
$E = \{k \mid \forall i < k,\ g(h_1(i)) < g(h_1(k))\}$.
Это множество разрешимо, бесконечно, и функция $g \cdot h_1$ на нем возрастает.

Пусть $h_2 : Z^+ \to E$ — возрастающая общерекурсивная биекция (см. то же предложение 5. 6. гл. I)

Тогда функция $h = h_1 \cdot h_2$ обладает требуемыми свойствами. Теорема доказана.

2.11. Замечания. а) Теорема 2.10 показывает, что вычисление сложности является творческой задачей: даже если мы нашли какой-то номер функции f в оптимальном семействе $\{u_k\}$, она могла бы встретиться еще раньше.

б) Так как $C(k) \neq C(l) \Rightarrow k \neq l$, то для всех x, B число $\{y \mid y \leqslant x, C(y) \leqslant \frac{x}{B}\} \leqslant \frac{x}{B}$, т. е. большинство чисел имеет большую сложность.

Тем не менее эффективно указать последовательность чисел асимптотически максимальной сложности невозможно. Точнее, пусть $\{k_i\}$ — любая возрастающая последовательность с $C(k_i) \geqslant \frac{k_i}{B}$ для некоторой константы B. Тогда нет ни одного перечислимого бесконечного множества E, содержащегося в $\{k_i\}$. Иначе мы могли бы найти возрастающую общерекурсивную функцию h: $Z^+ \to E$ и получить противоречие, как в теореме 2.10.

в) Пусть $u = \{u_k\}$ — любое оптимальное семейство m-функций. «Моменты первых появлений»

$$\{k \mid \forall i < k,\ u_i \neq u_k\}$$

образуют как раз последовательность асимптотически максимальной сложности, ибо по определению и п. 2.7б для них

$$k = C_u(u_k) \geqslant \text{const}\ C(k).$$

Таким образом, можно сказать, что в оптимальном семействе функции впервые появляются «в случайные моменты».

Задача вычисления $C(u_k)$ осложняется тем, что в версальных семействах любая функция появляется бесконечно часто, так что, если не повезет, она может быть впервые обнаружена как угодно далеко от места своего первого появления.

г) Укажем, наконец, что по крайней мере один существенный аспект сложности вычислений теорией понятия C_u не затрагивается: $\log_2 C(k)$ измеряет длину программы, необходимой для вычисления k, но не касается времени, в течение которого эта программа должна работать, не говоря уже о возможностях сокращения времени за счет параллелизации вычислений или удлинения программы и т. п. См. по этому поводу сборник [6] и цитированную там литературу.

Понятие сложности лежит на горизонте практической пользы. Однако оно кажется столь фундаментальным, что его роль в теоретической математике, возможно, еще будет возрастать.

3. СЛОЖНОСТЬ И СЛУЧАЙНОСТЬ

3.1. Мы несколько раз упоминали о том, что сложные последовательности «ведут себя, как случайные». С математической точки зрения корректной формулировке результата должно предшествовать определение случайной последовательности в терминах теории рекурсивности; разумеется, это определение должно удовлетворять естественным интуитивным условиям. Главная цель этого параграфа — сформулировать такое определение и некоторые точные результаты о связи сложности и случайности, которые можно доказать, пользуясь им.

3.2. Чтобы привлекать как можно меньше понятий теории вероятности, мы будем рассматривать в качестве пространства элементарных событий Ω множество бесконечных последовательностей из нулей и единиц с какой-нибудь вероятностной мерой P, например мерой Лебега L.

Если наблюдателю по очереди предъявляются члены последовательности, он может как-то отрабатывать начальные отрезки, стараясь найти в них «закономерности»: скажем, он может проверять последовательность на наличие периодичности, вычислять частоты появления нуля, единицы или групп знаков и т. п. Идеализацией этих представлений служит понятие об универсуме «тестов на случайность» F, который определяется следующим образом

P — тест на случайность есть общерекурсивная функция F на множестве конечных последовательностей нулей и единиц со значениями в Z^+, которая удовлетворяет условию: для каждого $m > 0$ *P-мера множества последовательностей* ω, *у которых существует начальный отрезок* $(\omega)_n$ с $F((\omega)_n) \geqslant m$, *не превосходит* 2^{-m}

Грубо говоря, функция F считает, на сколько бит закономерностей определенного типа можно найти в данной последовательности; каждый бит закономерностей должен по крайней мере вдвое урезать множество допустимых последовательностей. Требование общерекурсивности F обеспечивает возможность передачи проверки на случайность компьютеру. Положим

$$F(\omega) = \sup_n F((\omega)_n)$$

и будем говорить, что последовательность ω выдерживает тест F, если $F(\omega) < \infty$.

P — случайной последовательностью называется последовательность, выдерживающая все P-тесты.

Это определение было дано П. Мартином-Лефом на основе идей А. Н. Колмогорова (см. [21]). Приняв его, можно доказать, что все

случайные последовательности удовлетворяют всем эффективно проверяемым законам теории вероятностей, вроде закона больших чисел, повторного логарифма и т. п. Дело в том, что условие невыполнения закона можно переработать в тест, которого не выдерживают соответствующие последовательности. Если мера P в некотором (легко уточняемом) смысле слова вычислима, то можно построить один универсальный P-тест, заменяющий все тесты (ибо универсум P-тестов тогда перечислим).

3.3. Пусть $l(x)$ — длина двоичного слова x. Обозначим через $p(x)$ число бит закономерностей, которое найдет в нем универсальный L-тест U. Для определения $p(x)$ нужно применять U ко всем последовательностям длины n, начинающимся с x, вычислить наименьшее значение U на таких последовательностях и затем его максимум при $n \to \infty$. (В самом деле, универсальность теста есть «предельное» понятие и для отыскания закономерностей в x может потребоваться анализ продолжений x.)

Результат Мартина-Лефа, связывающий понятия сложности и случайности, дается следующим неравенством:

$$| l(x) - (p(x) + K(x)) | \leqslant 4l(l(x)) + \text{const}.$$

Грубо говоря, сложность числа плюс число бит закономерностей в его двоичном разложении по порядку почти совпадает с длиной двоичного разложения.

В частности, если последовательность ω случайна, то сложность $(\omega)_n$ не меньше, чем

$$n - 4l(n) + \text{const}$$

для всех n.

Глава IV

ФОРМАЛЬНЫЕ ЯЗЫКИ И ВЫЧИСЛИМОСТЬ

Эта глава служит подготовкой к изложению теоремы Геделя в гл. V. Здесь и ниже мы пользуемся определениями и обозначениями из Д и НД.

1. АРИФМЕТИКА СИНТАКСИСА

1.1. В этом параграфе показано, как синтаксис формальных языков в принципе сводится к арифметике. С этой целью символы, выражения, тексты в конечном или счетном алфавите A отождествляются с натуральными числами (нумеруются) таким образом, что синтаксические операции (соединения, подстановки и др.) представляются рекурсивными функциями, а синтаксические отношения (вхождение,

«быть формулой» и др.) прадставляются разрешимимы или перечислимыми множествами.

Наша первая забота — показать, что на множествах выражений и текстов вычислимость синтаксических операций и разрешимость (перечислимость) синтаксических отношений не зависят от способа нумерации, если только он подчинен слабым естественным ограничениям.

Эта независимость позволяет рассматривать метод нумерации не просто как технический прием, но как отражение глубинной эквивалентности арифметики и комбинаторики формальных текстов. В практике современных ЭВМ, где содержимое ячейки может быть неразъединенным сплавом числа, имени (кода) и команды, эквивалентность синтаксиса и арифметики реализована в «железе» и воспринимается как азы. Это было не так в 1931 году, когда появилась работа Геделя, введшая нумерацию в математический обиход.

Укажем, наконец, что с точки зрения психолога нумерация множества A есть простейший способ помечать его элементы различными метками $|$, $||$, $|||$, ... и т. п.

1.2. Нумерация. Пусть S — конечное или счетное множество. *Нумерацией* S мы назовем любое инъективное отображение $N : S \to Z^+$, образ которого *разрешим*. Число $N(s)$ называется *N-номером* элемента $s \in S$.

Нумерации N, $N' : S \to Z^+$ называются *эквивалентными*, если частичные функции $N \circ (N')^{-1}$, $N' \circ N^{-1} : Z^+ \to Z^+$ *частично рекурсивны*. Эти функции автоматически *вычислимы* (а не только полувычислимы), ибо их области определения разрешимы (см. § 1, 2 гл. I).

Эти и последующие определения имеют ясный интуитивный смысл: разрешимость множества номеров обеспечивает распознаваемость свойства «быть номером элемента S»; эквивалентность нумераций — эффективное восстановление одного номера по другому. В § 11 гл. II книги Д и НД описана конкретная нумерация множества выражений в языке арифметики Шмульяна S Ar. Заметим, что наше определение нумерации приспособлено специально к сравнению арифметики и синтаксиса и отличается от определения, принятого в книге [5], где нумерацией называется отображение $Z^+ \to S$. Мы отсылаем читателя к этой книге за изложением большого количества тонких результатов общей теории нумерации.

1.3. Лемма. а) *Эквивалентность нумераций является рефлексивным, симметричным и транзитивным отношением.*

б) *Любое инъективное отображение конечного множества в Z^+ является нумерацией, и любые две нумерации конечных множеств эквивалентны.*

в) *Любая нумерация бесконечного множества эквивалентна нумерации с образом Z^+.*

Все это очевидно или уже было доказано; в частности, в) следует из предложения 5.2. гл. I.

1.4. Пусть S_1, S_2 — два множества,
$N_i : S_i \to Z^+$, $i = 1, 2$,
их нумерации. Частичное отображение $f : S_1 \to S_2$ называется *частично рекурсивным относительно* $\langle N_1, N_2 \rangle$, если отображение $N_2 \circ f \circ N_1^{-1} : Z^+ \to Z^+$ частично рекурсивно. Тавтологический пример: отображение нумерации $N : S \to Z^+$ частично рекурсивно относительно $\langle N$, тождество$\rangle$.

Подмножество $T \subseteq S$ называется разрешимым, перечислимым, арифметическим относительно нумерации N_1, если множество $N_1(T)$ обладает соответствующим свойством.

1.5. **Лемма.** *Если в условиях п. 1.4. заменить* $\langle N_1, N_2 \rangle$ *на пару эквивалентных нумераций* $\langle N_1', N_2' \rangle$, *то классы рекурсивных отображений* $S_1 \to S_2$ *и разрешимых, перечислимых, арифметических подмножеств в* S_2 *не изменятся.*

Доказательство. Композиция вычислимых рекурсивных функций рекурсивна и вычислима. Прообраз разрешимого (соответственно перечислимого) множества относительно вычислимой функции разрешим (перечислим). Наконец, пусть $f : Z^+ \to Z^+$ — частично рекурсивная функция, $E \subseteq Z^+$ — арифметическое множество. Тогда $f^{-1}(E) = \mathrm{pr}_1((Z^+ \times E) \cap \Gamma_f)$ (в $Z^+ \times Z^+$). Так как $Z^+ \times E$ арифметично и Γ_f арифметично (даже диофантово), то и $f^{-1}(E)$ арифметично.

1.6. Пусть S_i — множества с нумерациями N_i, $i = 1, \ldots, r$. Нумерация $N : S_1 \times \ldots \times S_r \to Z^+$ называется *согласованной* с $\langle N_1, \ldots, N_r \rangle$, если для всех $i = 1, \ldots, r$ проекции $\mathrm{pr}_i : S_1 \times \ldots \times S_r \to S_i$ рекурсивны относительно $\langle N_1 N_i \rangle$ и частичная функция $(Z^+)^r (N_1^{-1}, \ldots, N_r^{-1}) S_1 \times \ldots \times S_r \xrightarrow{N} Z^+$ рекурсивна. Иными словами, N_i-номера координат вычисляются по N-номеру вектора и наоборот.

1.7. **Лемма.** а) *В обозначениях п. 1.5 для любых* $\langle N_1, \ldots, N_r \rangle$ *согласованная с ними нумерация N существует. Например, можно положить для* $s_i \in S_i$, $i = 1, \ldots, r$
$N(s_1, \ldots, s_r) = \tau^{(r)}(N_1(s_1), \ldots, N_r(s_r))$
(*определение* $\tau^{(r)}$ *см. в п. 4.5 гл. V*).

б) *Если N согласована с* $\langle N_1, \ldots, N_r \rangle$, *N эквивалентна N', Ni эквивалентны* N_i' $(i = 1, \ldots, r)$, *то N' согласована с* $\langle N_1', \ldots, N_r' \rangle$.

в) *Если N согласована с* $\langle N_1, \ldots, N_r \rangle$ *и N' согласована с* $\langle N_1, \ldots, N_r \rangle$, *то N и N' эквивалентны. Если N согласована с* $\langle N_1, \ldots, N_r \rangle$ *и с* $\langle N_1', \ldots, N_r' \rangle$, *то* N_i *и* N_i' *эквивалентны для всех* $i = 1, \ldots, r$.

Все это вместе означает, что сеймества из r классов нумераций множеств $S_1, \ldots, S_r$ (с точностью до эквивалентности) взаимно однозначно соответствуют некоторым классам нумераций $S_1 \times \ldots \times S_r$ (посредством отношения согласованности). Доказательство леммы сводится к механической проверке определений.

1.8. Пусть $A^l = A \times \ldots \times A$ (l раз) и $S(A) = A^0 \cup A^1 \cup \ldots \cup A^l \cup \ldots$ Если A — алфавит, то $S(A)$ — множество выражений в нем; $A^0 = \{\Lambda\}$ состоит из пустого выражения. Функция $S(A) \to Z^+$, принимающая значение p на A^p, есть *длина* выражения. Частичная функция «i-я координата» $Z^+ \times S(A) \to A^1 : \langle i, \langle a_1, \ldots, a_p \rangle\rangle \to a_i$ определена на подмножестве $\bigcup_{i=1}^{\infty} \{i\} \times (A^i \cup A^{i+1} \cup \ldots)$ Функция «соединение» $S(A) \times S(A) \to S(A)$ переводит $\langle\langle a_1, \ldots, a_p\rangle, \langle b_1, \ldots, b_q\rangle\rangle$ в $\langle a_1, \ldots, a_p, b_1, \ldots, b_q\rangle$.

Нумерация N множества $S(A)$ называется *допустимой*, если функции «длина», «i-я координата» и «соединение» частично рекурсивны относительно $\langle N, \mathrm{id}\rangle$, $\langle\langle \mathrm{id}, N\rangle, N\rangle$, $\langle\langle N, N\rangle, N\rangle$ соответственно.

Нумерация N множества $S(A)$ называется *согласованной с нумерацией* N_0 множества A, если она допустима и ограничение N на A^1 эквивалентно N_0 на A (при отождествлении A с A^1).

Вот основной результат этого параграфа:

1.9. Предложение. а) *Если N допустима, то любая эквивалентная ей нумерация допустима.*

б) *Если N и N_0 согласованы, N' эквивалентна N, N' эквивалентна N_0, то N' и N согласованы.*

в) *Если N и N_0 согласованы, N' и N_0 согласованы, то N и N' эквивалентны.*

г) *Для любой нумерации N_0 множества A существует согласованная с ней нумерация N множества $S(A)$, класс которой однозначно определен классом N_0 в силу* в).

Доказательство. а) и б) формально получаются с помощью леммы 1.6. Утверждение в) следует из того, что переход от N'-номера к N-номеру выражения происходит так.

Пусть $m * n = N(N^{-1}(m) N^{-1}(n))$ (под знаком N стоит соединение). Частичная операция $Z^+ \times Z^+ \to Z^+ : \langle m, n\rangle \to m * n$. рекурсивна и ассоциативна в силу допустимости N.

Пусть далее $(k)_i = N$ (i-я координата $N^{-1}(k)$). Частичная операция $Z^+ \times Z^+ \to Z^+ : \langle k, i\rangle \to (k)_i$; рекурсивна по той же причине. Аналогично определяется $(k)'_i$ по N'.

Наконец, пусть l': $Z^+ \to Z^+$ — частичная функция «длина $N'^{-1}(k)$». Она также рекурсивна.

Тогда имеем

$$N \circ N'^{-1}(k) = N \circ N'^{-1}((k)'_1) * \ldots * N \circ N'^{-1}((k)'_{l'(k)}).$$

Но N'-номера однобуквенных выражений $\{(k)'_i\}$ составляют разрешимое подмножество в Z^+ (1-уровень вычислимой функции l'). Ограничение $N \circ N'^{-1}$ на это подмножество является рекурсивной функцией, ибо ограничения N и N' на A^1 эквивалентны. Отсюда и из рекурсив-

ности $*$, $(k)_i'$ и l' получается в) (рекурсия по x для $x \underset{i=1}{\overset{*}{N}} N'^{-1}((k)_i')$ и подстановка $x = l'(k)$).

Утверждение г) мы установим с помощью явной конструкции Геделя (идея ее, впрочем, восходит к Лейбницу).

1) *Конструкция N, согласованной с N_0:*

$$N(a_1, \ldots, a_m) = p_1^{N_0(a_1)} \ldots p_m^{N_0(a_m)},$$

где $p_1 = 2$, $p_2 = 3$, ... — последовательные простые числа; $N(\Lambda) = 1$.

Проверим, удовлетворяет ли N всем требованиям.

г$_2$) N является нумерацией. То, что $N : S(A) \to Z^+$ вложение, следует из того, что $N_0 : A \to Z^+$ вложение и из теоремы об однозначном разложении в Z^+.

Установим разрешимость образа N. Прежде всего множество простых чисел в Z^+ разрешимо как 2-уровень всюду определенной рекурсивной функции $n \to$ число делителей $n = \sum\limits_{k=1}^{n} d(k, n) - n$, где (см. § 3 гл. I)

$$d(k, n) = s((\mathrm{rem}(k, n) - k)^2 + 1) = \begin{cases} 2, & \text{если } k/n, \\ 1 & \text{в противном случае.} \end{cases}$$

$s(1) = 2$, $s(\geqslant 2) = 1$.

Поэтому функция $i \to p_i$ рекурсивна (см. доказательство предложения 5.2 гл. I).

Положим теперь

$$f(n, i, y) = s((\mathrm{rem}(p_i^y, n) - p_i^y)^2 + 1).$$

Эта функция рекурсивна, поэтому рекурсивна по (n, i) также $v_i(n) = \min\{y \mid f(n, i, y) = 1\}$ = (степень, в которой p_i делит n) + 1. Отсюда следует, что рекурсивна «длина»: $l(n)$ = число простых делителей $n = \sum\limits_{i=1}^{n} s(v_i(n)) \dot{-} n$ (заведомо $p_m \neq n$ при $m > n$, ибо $p_m > m$).

Пусть теперь E — образ N_0 в Z^+. Тогда образ $N = \{n \mid \forall i \leqslant l(n),\ v_i(n) \in E + 1\}$.

Применение ограниченного квантора общности не портит разрешимости. Действительно, пусть $F = \{\langle i, n\rangle \mid v_i(n) \in E + 1\}$. F разрешимо как v-прообраз E. Пусть $\chi_F(i, n) = 1$ при $\langle i, n\rangle \in F$, $\chi_F(i, n) = 2$ при $\langle i, n\rangle \notin F$. Функция $s\left(\prod\limits_{i=1}^{l(n)} \chi_F(i, n)\right)$ от n имеет своим 2-уровнем образ N.

г$_3$) *N допустима.* Рекурсивность «длины» мы уже проверили. «i-я координата» представляется функцией

$$\left[p_i^{v_i(n)}/p_i\right] \text{ (целая часть).}$$

Наконец, соединение представляется функцией

$$m * n = m \prod_{i=1}^{(n} p^{\circ_i (n)_{-1}}_{(m)+1},$$

рекурсивность которой следует из уже доказанных фактов.

Заметим, что наши арифметические функции определены не только на множествах геделевых номеров любой конкретной нумерации, но на всем Z^+. В дальнейшем такое расширение областей определения мы не будем отмечать без особой необходимости

г$_4$) N *согласована* с N_0. На однобуквенных выражениях переход от одной нумерации к другой задается функциями $x \to 2^x$, $y \to \log_2 \cdot (y)$ $(y \in 2^{Z^+})$, рекурсивность которых очевидна.

На этом заканчивается доказательство предложения 1.9.

1.10. Заключительные замечания. Предложение 1.9 показывает, что если задан класс эквивалентных нумераций алфавита A формального языка; то однозначно определен класс эквивалентных нумераций множества выражений $S(A)$, множество текстов $S(S(A))$ и т. д., согласованных с нумерациями A из этого класса. Поэтому множества рекурсивных операций и разрешимых или перечислимых отношений на выражениях и текстах определены инвариантно.

Единственная оставшаяся неоднозначность — выбор класса эквивалентных нумераций A.

Во всех известных автору случаях этот выбор также канонически определяется следующим образом: *A реализуется как разрешимое подмножество выражений некоторого конечного «протоалфавита» A_0*; при этом разрешимость понимается в смысле любой нумерации $S(A_0)$, согласованной с любой нумерацией A_0. В силу лемм 1.3, 1.5 и предложения 1.9, примененных к A_0, полученный класс нумераций A уже не будет зависеть ни от вложения A в $S(A_0)$, ни от нумерации A_0, ни даже от выбора A_0 (учесть, что если $A_0 \subset A_1$ конечны, то $S(A_0) \subset S(A_1)$ разрешимо).

Описанный в § 10 гл. II книги Д и НД девятибуквенный алфавит языка S Ar с нынешней точки зрения естественнее считать протоалфавитом: выражения x, x', x'', x''', ... суть элементы «настоящего алфавита». Нумерация Шмульяна очень удобна для доказательства теоремы Тарского, но «невыразимость истинности» в S Ar от ее конкретного вида не зависит: теперь это должно быть совершенно ясно.

Более общо, любое полное печатное описание любого алфавита A реализует A в протоалфавите наличных типографских знаков, который, разумеется, конечен, и тем определяет канонический класс эквивалентных нумераций A.

2. СИНТАКСИЧЕСКИЙ АНАЛИЗ

2.1. В этом параграфе собран подготовительный технический материал для § 3, в котором устанавливается перечислимость вводимых формул в языках $\mathscr{L}_1$ (см. Д и НД).

Пусть L — фиксированный язык класса $\mathscr{L}_1$ с конечным или счетным алфавитом A. Для некоторого сокращения технической работы ограничимся диалектом со связками $\neg$, $\to$ и квантором $\forall$. Это ни в каких отношениях не существенно. Предполагается, что на A задан канонический класс эквивалентных нумераций, как в § 1, который определяет нумерации $S(A)$, $S(S(A))$ и т. п. Рекурсивность, разрешимость и т. д. понимаются относительно этого класса. В формулировках основных результатов поэтому мы вправе не упоминать нумерацию явно. В доказательствах, однако, удобнее работать прямо с номерами. Поэтому мы фиксируем одну из нумераций $N : S(A) \to Z+$ с функциями соединения $*$, длины l и i-й координаты $(k)_i$, как в доказательстве предложения 1.9. Будем считать, что $m * n > \max(m, n)$: номер любой части выражения строго меньше номера целого. Нумерация Геделя именно такова.

Дополнительно к условиям § 1 мы потребуем, чтобы N удовлетворяла следующим условиям распознаваемости синтаксических характеристик символов алфавита:

а) *Множества переменных, констант, операций и отношений в A разрешимы.*

б) *Функция «ранг» на множестве операций и отношений рекурсивна.*

Теперь мы можем приступить к делу. Перед чтением дальнейшего рекомендуется просмотреть § 1 гл. II.

2.2. *Частичное отображение $S(A) \times Z+ \to Z+ : \langle$выражение P, $i \rangle \mapsto$ номер места скобки), парной к скобке (, стоящей на i-м месте в выражении P вычислимо, т. е. рекурсивно с разрешимой областью определения.*

Доказательство. Нам будет удобно пользоваться следующим обозначением: если Q — некоторое высказывание о целых числах из $Z+$, то

$$\|Q\| = \begin{cases} 1, & \text{если } Q \text{ истинно,} \\ 2, & \text{если } Q \text{ ложно.} \end{cases}$$

Это функция истинности, приспособленная к отсутствию нуля в $Z+$.

Построим функцию Par $(k, i) : Z+ \times Z+ \to Z+$

$$\mathrm{Par}(k, i) = \begin{cases} 1, \text{ если } (k)_i \text{ не определено, или } (k)_i \neq N(\text{(}); \\ \text{или } (k)_i = N(\text{(}), \\ \text{но } \forall j \in [i, l(k)], \\ \sum\limits_{m=i}^{j} \|(k)_m = N(\text{(})\| \neq \sum\limits_{m=i}^{j} \|(k)_m = N(\text{)})\|; \\ \min\{j \mid j \leqslant l(k)\} \text{ и } \sum\limits_{m=i}^{j} \|(k)_m = N(\text{(})\| = \\ = \sum\limits_{m=i}^{j} \|(k)_m = N(\text{)})\| \text{ в противном случае.} \end{cases}$$

Очевидно, после ограничения на $N^{-1}(S(A)) \times Z+$ функция Par (k, i) даст номер места парной скобки k, стоящей на i-м месте в выражении $N^{-1}(k)$, когда это возможно, и 1, когда это невозможно (см. лемму 1.2 § 1 гл. II книги Д и НД). Поэтому достаточно установить рекурсивность Par (k, i).

Но написанное определение функции Par (k, i) представляет ее в виде склейки конечного числа (четырех) рекурсивных функций с разрешимыми (в силу свойств N) областями определения. Поэтому она рекурсивна.

2.3. *Частичное отображение $S(A) \to Z+$ (выражение P) $\to$ (число термов L, соединением которых является P) вычислимо.*

Напомним, что это число определено однозначно (§ 1 гл. II).

Доказательство. Мы построим сначала формулу, которая рекурсивно определяет функцию $Z+ \to Z+$

$l\,T(k) = \{l(k) + 1$, если $N^{-1}(k)$ не есть соединение термов; число термов, соединение которых есть $N^{-1}(k)$ в противном случае — через ее значения для меньших значений аргумента. Словесный рецепт для синтаксического анализа $N^{-1}(k)$ таков: нужно посмотреть, является ли $(k)_1$ переменной или константой и если да, то является ли $(k)_2 * \ldots * (k)_{l(k)}$ соединением термов; если нет, является ли $(k)_1$ операцией, стоит ли за ней скобка «(», есть ли к ней парная скобка »)», стоит ли после »)» соединение термов (В предыдущей фразе названы номера вместо выражений.)

Для систематического описания положим

$$f_1(k) = \begin{cases} (k)_2 * \ldots * (k)_{l(k)}, & \text{если } l(k) \geqslant 2; \\ 1 \text{ — в противном случае;} \end{cases}$$

$$f_2(k) = \begin{cases} (k)_3 * \ldots * (k)_{\mathrm{Par}(k,2)-1}, & \text{если } 4 \leqslant \mathrm{Par}(k, 2); \\ 1 \text{ — в противном случае;} \end{cases}$$

$$f_3(k) = \begin{cases} (k)_{\mathrm{Par}(k,2)+1} * \ldots * (k)_{l(k)}, & \text{если } 1 < \mathrm{Par}(k, 2) < l(k); \\ 1 \text{ — в противном случае.} \end{cases}$$

Все эти функции рекурсивны.

Теперь можно написать следующий рецепт для рекурсивного вычисления $LT(k)$:

$$l(k) = 1 \text{ и } \begin{cases} N^{-1}(k) \text{ переменная} & \Rightarrow LT(k) = 1, \\ N^{-1}(k) \text{ константа} & \Rightarrow LT(k) = 1, \\ N^{-1}(k) \text{ ни то, ни другое} & \Rightarrow LT(k) = 2; \end{cases}$$

$$l(k) > 1 \text{ и } \begin{cases} N^{-1}((k)_1) \text{ переменная} \Rightarrow LT(k) = 1 + LT(f_1(k)), \\ N^{-1}((k)_1) \text{ константа} \Rightarrow LT(k) = 1 + LT(f_1(k)), \\ N^{-1}((k)_1) \text{ операция}, (k)_2 = N(\,(\,), 4 < \mathrm{Par}(k, 2) = l(k), \\ \qquad \text{ранг } N^{-1}((k)_1) = LT(f_2(k)) \leqslant l(f_2(k)) \Rightarrow \\ \qquad\qquad \Rightarrow LT(k) = 1; \end{cases}$$

$l(k) > 1$ и $(N^{-1}(k)_1)$ — операция, $(k_2) = N((), 4 < \mathrm{Par}(k, 2) < l(k)$, ранг $N^{-1}((k)_1) = LT(f_2(k)) \leqslant l(f_2(k))$, $LT(f_3(k)) < l(f_3(k)) \Rightarrow LT(k) = 1 + LT(f_3(k))$;
$l(k) > 1$ и ни одно из предыдущих (сложных) условий не выполнено $\Rightarrow LT(k) = 1 + l(k)$.

Чтобы установить рекурсивность LT, заметим сначала, что для каждой из выписанных восьми альтернатив легко построить рекурсивную функцию $h_i(k, x, y, z)$ со следующим свойством:
$\|k$ удовлетворяет i-й альтернативе$\| \Rightarrow$
$\Rightarrow h_i(k, LT(f_1(k)), LT(f_2(k)), LT(f_3(k)))$,

а также рекурсивную функцию $v_i\ (k, x, y, z)$ со свойством (k удовлетворяет i-й альтернативе) $\Rightarrow LT\ (k) = v_i\ (k, LT\ (f_1\ (k)), LT\ (f_2, (k)), LT\ (f_3\ (k)))$.
Поэтому справедливо равенство

$$LT\ (k) = 2 \sum_{i=1}^{8} v_i\ (k, LT\ (f_1\ (k)), LT\ (f_2\ (k)),$$

$$LT\ (f_3\ (k))) = \sum_{i=1}^{8} (h_i\ v_i)\ (k, LT\ (f_1\ (k)),$$

$$LT\ (f_2\ (k)), LT\ (f_3\ (k))).$$

Вместе с $LT\ (1)$ эта формула позволяет реально вычислять последовательно значения $LT\ (k)$, ибо $f_i\ (k) < k$ при $k > 1$. Но рекурсия при этом происходит не к предыдущему значению k, а к нескольким из рассмотренных ранее. Это и есть основная трудность установления рекурсивности синтаксических функций. Мы покажем сейчас, как она преодолевается в этом и во всех последующих случаях

Пусть вообще $\varphi_1\ (k), \ldots, \varphi_s\ (k)$ — рекурсивные функции со свойством: для всех $i \leqslant s$ и $k \geqslant 2$, $\varphi_i\ (k) < k$. Пусть далее $h\ (x_1, \ldots, x_n, k, y_1, \ldots, y_s)$ — рекурсивная функция и пусть $g\ (x_1, \ldots, x_n, k)$ определена соотношениями

$g\ (x_1, \ldots, x_n, k) =$ известная рекурсивная функция;
$g\ (x_1, \ldots, x_n, k + 1) = h\ (x_1, \ldots, x_n; k; g\ (x_1, \ldots, x_n, \varphi_1\ (k)), \ldots, g\ (x_1, \ldots, x_n, \varphi_s\ (k)))$.

Пользуясь функцией соединения $*$, положим

$$G\ (x_1, \ldots, x_n, k) = \mathop{*}_{i=1}^{k} g\ (x_1, \ldots, x_n, i).$$

Так как

$$g\ (x_1, \ldots, x_n, i) = (G\ (x_1, \ldots, x_n, k))_i$$

для всех $i \leqslant l\ (G\ (x_1, \ldots, x_n, k)) = k$, в частности, для наибольшего такого i, то для проверки рекурсивности g достаточно установить рекурсивность G. Но для G имеем при $k \geqslant 2$

$$G\ (x_1, \ldots, x_n, k + 1) = G\ (x_1, \ldots, x_n, k) *$$
$$g\ (x_1, \ldots, x_n, k + 1) = G\ (x_1, \ldots, x_n, k) *$$
$$h\ (x_1, \ldots, x_n; k; (G\ (x_1, \ldots, x_n, k))_{\varphi_1(k)}, \ldots,$$
$$(G\ (x_1, \ldots, x_n, k))_{\varphi_n(k)}),$$

что является стандартным рекурсивным уравнением.

Применяя этот трюк к LT, получаем ее рекурсивность: здесь $n = 0$, $s = 3$ и $\varphi_i\ (k) = f_i\ (k + 1)$.

Следствие. *Множество термов разрешимо.*

Действительно, это 1-уровень вычислимой функции LT.

2.4. *Множество атомарных формул разрешимо.*

Действительно,

$N^{-1}(k)$ атомарная формула $\Longleftrightarrow (k)_1$ отношение, $(k)_2 = N\ (0, \text{Par}\ (k, 2)) = l\ (k) \geqslant 4$, ранг $N^{-1}\ ((k)_1) = LT\ (f_2\ (k)) \leqslant l\ (f_2\ (k))$, где $f_2\ (k)$ определена в предыдущем пункте.

2.5. *Множество формул разрешимо.*

Действительно, в нашем упрощенном диалекте имеем: $N^{-1}\ (k)$ формула $\Longleftrightarrow N^{-1}\ (k)$ есть атомарная формула, или $\neg\ (P)$, или $(P) \to Q$ или $\forall\ x\ (P)$, где P, Q — формулы; x — переменная.

По образцу п. 2.3 определяем рекурсивные функции

$$f_4(k)=\begin{cases}(k)_3 * \ldots * (k)_{l(k)-1}, & \text{если } l(k)>4,\\ 1 \text{—в противном случае.}\end{cases}$$

$$f_5(k)=\begin{cases}(k)_2 * \ldots * (k)_{\mathrm{Par}(k,\,1)-1}, & \text{если } \mathrm{Par}(k,\,1)>3,\\ 1 \text{—в противном случае;}\end{cases}$$

$$f_6(k)=\begin{cases}(k)_{\mathrm{Par}(k,\,1)+3} * \ldots * (k)_{l(k)-1}, & \text{если } 3 \leqslant \mathrm{Par}(k,\,1) \leqslant l(k)-4,\\ 1 \text{—в противном случае;}\end{cases}$$

$$f_7(k)=\begin{cases}(k)_4 * \ldots * (k)_{l(k)-1}, & \text{если } l(k)>5,\\ 1 \text{—в противном случае;}\end{cases}$$

$$At(k)=\begin{cases}1, & \text{если } N^{-1}(k) \text{—атомарная формула,}\\ 2 \text{—в противном случае.}\end{cases}$$

Функция

$$F_m(k)=\begin{cases}1, & \text{если } N^{-1}(k) \text{—формула,}\\ 2 \text{—в противном случае}\end{cases}$$

вычисляется с помощью рекурсивного соотношения

$(\ s(1)=1,\ s(k)=2 \text{ при } k>2\ )$

$F_m(k)=s \circ \min\{At(k);\ \|(k)_1=N(\neg)\| \cdot \|k_1=N(\ (\ )\| \times \|l(k)>4\| \circ Fm(f_4(k))\};$

$(k)_1=N(\ (\ )\| \circ \|\mathrm{Par}(k,\,1)>3\| \circ Fm(f_5(k)) \times \|(k)_{\mathrm{Par}(k,\,1)+1}=$

$=N(\to)\| \circ \|(k)_{\mathrm{Par}(k,\,1)+2}=N(\ (\ )\| \circ \mathrm{Par}(k,\,\mathrm{Par}(k,\,1)+2)=l(k)\| \times Fm(f_6(k))\};$

$(k)_1\|=N(\forall)\| \circ \|(k)_2=N\ (\text{переменная})\| \circ \|(k)_3=N(\ (\ )\| \times \|\mathrm{Par}(k,\,3)=$

$=l(k)>3\| \circ Fm(f_7(k))\}.$

Рекурсивность $F_m(k)$ теперь устанавливается с помощью приема, описанного в п. 3.3.

Следствие. *Множества формул вида* $\neg(P)$, $(P) \to (Q)$, $\forall x\,(p)$ *разрешимы.*

2.6. *Отображение* $S(A) \times Z+ \times S(A) \to S(A)$: $\langle P,\ i,\ Q\rangle \mapsto$ *результат подстановки* P *вместо* i*-го символа в выражении* Q *вычислимо.*

Положим

$$\mathrm{Sub}(k,\,l,\,m)=\begin{cases}(m)_1 * \ldots * (m)_{i-1} * k * (m)_i * \ldots * (m)_{l(m)}, & \text{если } l \leqslant l(m),\\ 1 \text{— в противном случае.}\end{cases}$$

Ясно, что эта функция рекурсивна и на множестве $\langle k,\ l,\ m\rangle$ с $k,\ m \in N^{-1}(S(A))$ совпадает с требуемым отображением.

2.7. Отношение в $Z+ \times S(A) \times S(A)$: «*на* i*-м месте в формуле* P *стоит свободная переменная (однобуквенное выражение)* x» *разрешимо.*

Действительно, положим

$$\mathrm{Fr}(i,\,k,\,l)=\begin{cases}1, & \text{если условие 2.7 выполнено для } P=N^{-1}(k),\ \langle x\rangle=N^{-1}(l),\\ 2 \text{—в противном случае.}\end{cases}$$

Тогда имеем

$$\left.\begin{array}{l} N^{-1}(k) \text{ не формула, или } N^{-1}(l) \text{ не переменная,} \\ \text{или } i > l(k) \end{array}\right\} \Rightarrow \mathrm{Fr}(l, k, l) = 2.$$

Пусть теперь одновременно N^{-1} формула, $N^{-1}(l)$ переменная, $i < l(k)$.

Дальнейшие альтернативы:

$l \neq (k)_i \Rightarrow Fr(i, k, l)) = 2;$

$l = (k)_i,\ At(k) = 1 \Rightarrow Fr(i, k, l) = 1;$

$l = (k)_i,\ N^{-1}(k)$ имеет вид $\neg(P) \Rightarrow \mathrm{Fr}(l, k, l) = Fr(l, f_5(k), l)$;

$l = (k)_i,\ N^{-1}(k)$ имеет вид $(P) \to (Q),\ i < \mathrm{Par}(k, 1) \Rightarrow \mathrm{Fr}(i, k, l) =$

$= Fr(i, f_6(k), l);$

$l(k)_i,\ N^{-1}(k)$ имеет вид $(P) \to (Q),\ i > \mathrm{Par}(k, 1) + 2 \Rightarrow \mathrm{Fr}(i, k, l) =$

$= \mathrm{Fr}(i, f_6(k), l);$

$l(k)_i,\ N^{-1}(k)$ имеет вид $\forall x(P),\ (k)_2 \to l \Rightarrow \mathrm{Fr}(i, k, l) = 2;$

$l(k)_i,\ N^{-1}(k)$ имеет вид $\forall x(P),\ (k)_2 \neq l \Rightarrow \mathrm{Fr}(i, k, l) = \mathrm{Fr}(i, f_7(k), l).$

Функции $f_5, \ldots, f_7$ определены в п. 2.5. Дальше для доказательства рекурсивности Fr можно применить тот же прием, что в п. 2.4 и 2.5.

2.8. *Множество* $\{\langle x, P, t\rangle \mid x$ *переменная,* P *формула,* t *терм,* x *не связывает* t *в* $P\}$ *разрешимо.*

Это значит для номеров $\langle i, k, m\rangle$

$$\forall j \leqslant l(k) \left\{\begin{array}{l} \text{либо } (k)_j \neq i;\ \text{либо } (k)_j = i \wedge \mathrm{Fr}(j, k, i) = 2; \\ \text{либо } (k)_j = i \wedge \mathrm{Fr}(j, k, i) = 1 \wedge \forall n \in [1, l(m)] \times \\ \times\ |\mathrm{Fr}(j + n) \dot{-} 1,\ \mathrm{Sub}(m, j, k), \\ \mathrm{Sub}(m, j, k)_{j+n \dot{-} 1}) = \|(m)_n \text{ переменная } \|), \end{array}\right.$$

т. е. после подстановки t вместо любого свободного вхождения x в P все переменные в t остаются свободными.

2.9. *Частичное отображение* $\langle x, P, t\rangle \to$ *результат подстановки* t *вместо всех свободных вложений* x *в* P *вычислимо.*

Пусть $\langle i, k, m\rangle$ — номера x, P, t. Положим

$$f(j, k, t, m) = \left\{\begin{array}{ll} (k)_j, & \text{если } \mathrm{Fr}(j, k, i) = 2, \\ m, & \text{если } \mathrm{Fr}(j, k, i) = 1. \end{array}\right.$$

Это рекурсивная функция; и далее

$$\mathrm{Sub}\, t(i, k, m) = \overset{(k)}{\underset{j=1}{*}} f(j, k, t, m).$$

Это — номер результата подстановки t вместо всех свободных вхождений x в P.

3.1. Общая схема. Пусть L — произвольный язык с нумерованным счетным алфавитом A. Предположим, что фиксированы следующие данные:

а) Перечислимое множество «аксиом» $Ax \subset S(A)$.

б) Частично рекурсивное отображение $\mathrm{Inf}: Z^+ \times S(S(A)) \to S(A)$ — перечислимое семейство «правил вывода»

Будем говорить, что выражение $P \in S(A)$ *непосредственно следует из выражений* $P_1, \ldots, P_r$ *согласно* i*-му правилу вывода, если*

$$< i_1 < P_1, \ldots, P_r \gg \in D(\mathrm{Inf}) \text{ и } \mathrm{Inf}(i, < P_1, \ldots, P_r >) = P.$$

Назовем выражение P *выводимым* (из «аксиом»), если существует такая конечная последовательность выражений $P_1, \ldots, P_n = P$, что для каждого $j \leqslant n$ либо $P_j \in Ax$, либо существуют $i \in Z^+$ и $\{P_1, \ldots, P_r\} \subseteq \{P_1, \ldots, P_{j-1}\} \cup Ax$ такие, что P_j непосредственно следует из $P_1, \ldots, P$ согласно i-му правилу вывода.

Обозначим через D множество всех выводимых выражений.

3.2. Предложение. *D перечислимо.*

Доказательство. Пусть $a: Z^+ \to S(A)$ — рекурсивная функция, образ которой совпадает с Ax; $\inf: Z^+ \to S(A)$ — частично рекурсивная функция

$$\inf(n) = \mathrm{Inf}(t_1^{(2)}(n), N_1^{-1}(t_2^{(2)}(n))),$$

где $N_1: S(S(A)) \to Z^+$ — какая-нибудь нумерация текстов, согласованная с нумерацией выражений

Построим рекурсивную функцию $d: Z^+ \to S(A)$:

$$d(2n-1) = a(n);$$
$$d(2n) = \inf(n),\ n \geqslant 1.$$

Утверждается, что ее образ равен D. Действительно, достаточно проверить, что:

а) $Ax \subset$ образ d; б) если $P_1, \ldots, P_r \in$ образ d и P непосредственно следует из $P_1 \ldots, P_r$ по i-му правилу вывода, то $P \in$ образ d.

Но а) очевидно: все аксиомы выписываются на нечетных шагах. Для проверки б) выберем n так, что

$$t_1^{(2)}(n) = i,\ t_2^{(2)}(n) = N_1(<P_1, \ldots, P_r>).$$

Тогда $d(2n) = P$. Предложение доказано.

Проверим теперь, что эта общая ситуация реализуется в языках класса $\mathcal{L}_1$.

3.3. Правила вывода Gen и MP. Определим отображение $\mathrm{Inf}: Z^+ \times S(S(A)) \to S(A)$ так:

$$D(\mathrm{Inf}) = \{<1, <P, (P) \to (Q) \gg P, Q, \text{ формулы}\} \cup \{<i, <P \gg \mid P \text{ формула}, i \geqslant 2\},$$

$$\mathrm{Inf} < 1, <P\ (P) \to (Q) \gg = Q,$$

$$\mathrm{Inf}\langle i, \langle P\rangle\rangle = \forall x_{i-1}(Q),$$

где x_j — j-я переменная языка L в какой-нибудь фиксированной нумерации переменных с образом Z^+, согласованной с нумерацией A. Ясно, что Inf рекурсивно и исчерпывает правила вывода MP и Gen.

3.4. Аксиомы. Проверим, что в любом языке класса $\mathscr{L}_1$ перечислимы следующие множества:

а) тавтологии;

б) логические аксиомы с кванторами;

в) аксиомы равенства.

Кроме того, перечислимы

г) специальные аксиомы L_1 Ar;

д) специальные аксиомы L_1 Set. На самом деле все эти множества даже разрешимы, что нетрудно установить методами § 2, но перечислимость доказывается немного короче, и нам ее достаточно.

3.5. Тавтологии. В § 5 гл. II книги Д и НД построен конечный список схем базисных тавтологий и показано, что все остальные выводятся из них посредством MP. Поэтому согласно предложению 3.1 достаточно проверить перечислимость базисных тавтологий. Любая схема базисной тавтологии определяет множество формул вида

$$Q_1 P_{i_1} Q_2 P_{i_2} \ldots P_{i_r} Q_{r+1},$$

где Q_i — фиксированные непустые выражения (кроме, возможно, Q_1, Q_{r+1}); $i_1, \ldots, i_r \in \{1, \ldots, m\}$ и $\langle P_1, P_m \rangle$ пробегает упорядоченные m-ки формул L. Так как согласно п. 2.5 множество таких m-к разрешимо и операция соединения рекурсивна, ясно, что мы получаем перечислимое множество формул.

3.6. Аксиомы с кванторами. В диалекте $\mathscr{L}_1$, где $\exists$ исключен, они укладываются в две схемы аксиом:

а) $(\forall x\ (P\ (x))) \to (P\ (t))$, где x не связывает терм t в формуле P.

б) $(\forall x\ ((P) \to (Q))) \to ((P) \to (\forall x\ (Q)))$, если x не входит свободно в Q.

Согласно п.2.8 множество троек $\{\langle x, P, t\rangle \mid x$ не связывает t в $P\}$ разрешимо. Согласно п. 2.9 отображение $\langle x, P, t\rangle \to P\ (t)$ рекурсивно. Так как соединение тоже рекурсивно, множество аксиом а) перечислимо как образ разрешимого множества относительно рекурсивной функции.

Аналогично получится перечислимость б), если мы проверим, что условие «x не входит свободно в Q» разрешимо. Но оно равносильно, например, такому: «результаты подстановки в Q вместо свободных вхождений x переменных x_1, x_2 совпадают с Q», где x_1, x_2 — любая фиксированная пара переменных. Разрешимость этого условия следует из п. 2.9.

3.7. Аксиомы равенства. Согласно предложению 4,6 гл. II книги Д и НД достаточно проверить перечислимость формул вида

$$(x = y) \to (P\ (x,\ x) \to P\ (x,\ y)),$$

где P пробегает атомарные формулы языка, а $P(x, y)$ получается из P заменой любой части вхождений x на y; x, y — переменные. Их множество можно получить, например, как образ частично рекурсивной функции $S(A) \times A^1 \times A^1 \times S(Z^+) \to S(A)$:
$\langle P, \langle x\rangle, \langle y\rangle, \langle i_1, \ldots, i_r \rangle\rangle \to$ результат подстановки y на места $i_1, \ldots, i_r$ в атомарной формуле P, если на этих местах стоит x.
Рекурсивность ее следует из результатов п.2.4. и 2.6

3.8. **Аксиомы** $L_1\mathrm{Ar}$ и L_1 Set. Часть из них не содержит «метаязыковых переменных» для формул, а только переменные языка: это все аксиомы арифметики, кроме индукции, и все аксиомы теории множеств, кроме подстановки. Разрешимость каждого из множеств таких аксиом следует из того, что его можно описать условием типа «множество формул длины 39, у которых на 1-м месте стоит (, на 2-м $\forall$, на 3-м переменная, на 4-м (, ..., на 39-м), на 40-м); на 3-м, 8-м и 16-м местах переменные одинаковы; на 9-м и 36-м местах переменные одинаковы; на 17-м и 37-м местах переменные одинаковы; эти три переменные попарно разные» (аксиома объемности L_1Set в нормализованной записи). Впрочем, достаточно было бы написать по одному экземпляру каждой такой аксиомы: остальные порождаются Gen, аксиомой специализации и MP.

Перечислимость аксиом индукции и подстановки получается с помощью тех же приемов, что и перечислимость базисных тавтологий и логических аксиом с кванторами. Мы оставляем детали читателю.

Глава V

ТЕОРЕМА ГЕДЕЛЯ

1. ПРИНЦИП НЕПОЛНОТЫ

1.1. Теорема Геделя о неполноте формальных теорий может быть точно сформулирована во многих конкретных вариантах, ни один из которых не исчерпывает ее содержания целиком. В этом параграфе мы попытаемся отделить принципиальную сторону теоремы от технических деталей ее доказательств для разных языков, опираясь на результаты гл. IV.

1.2. Пусть A — конечный или счетный алфавит с каноническим классом нумерации; $S(A)$ — множество выражений над A. Предположим, что в $S(A)$ как-то определены два подмножества:

а) $T \subset S(A)$ — множество «истинных» выражений. Например, над A может быть задан язык, та или иная его семантика и функция истинности относительно нее.

б) $D \subset S(A)$ — множество «доказуемых» или «выводимых» выражений.

Оно может быть описано «аксиомами» или «правилами вывода» или как-нибудь еще. Мы будем считать, что $D \subseteq T$ в соответствии с семантикой терминов (доказуема лишь истина).

Есть все основания верить, что если D, T построены «естественно» в ходе любой формализации любого фрагмента современной математики, то выполняются следующие принципы.

1.3. *Множество D перечислимо*

Интуитивные аргументы в пользу этого таковы. Предположим, что «доказуемые» выражения — это те, для которых существуют «доказательства». «Доказательства» — это тексты, которые пишутся, возможно, в другом алфавите B, т. е. элементы $S(S(B))$. (Например, теоремы $L_1\mathrm{Ar}$ могут доказываться в языке L_1 Set.) Минимальное требование к формальным математическим доказательствам состоит в том, что бы они могли быть механически распознаваемы как таковые, т. е. образовывали разрешимое подмножество $S(S(B))$. (Впрочем, здесь было бы достаточно потребовать перечислимости и самих «доказательств».) Второе неизбежное требование состоит в том, чтобы по каждому «доказательству» можно было механически получить «доказанное выражение» в $S(A)$. Иными словами, частичная функция $S(S(B)) \to S(A)$: «доказательство» $\to$ «доказанное» должна быть (полу) вычислима. Но тогда ее образ перечислим.

В § 3 гл. IV мы установили перечислимость выводимых формул в языках α_1 в согласии с этими неформальными рассуждениями.

Заметим, что во всем обсуждении неявно присутствовал временной аспект: «доказательство» понимается как «доказательство с помощью средств, принятых к настоящему моменту и (полу) распознаваемых как таковые». После введения, скажем, новой аксиомы теории множеств и ее достаточно широкого признания понятие доказательства расширится, как это произошло с аксиомой выбора (или, скорее, принципом трансфинитной индукции, леммой Цорна...). Ср. с обсуждением в § 5.

1.4. *Множество T неперечислимо, если семантика истинности настолько богата, что включает в себя элементарную арифметику.*

Ясно, что мы имеем в виду те или иные варианты теоремы Тарского, доставляющие даже неарифметичность T. В соедующем параграфе мы укажем несколько точных конкретизаций этого принципа. См. также п. 5.3, 5.4 ниже.

1.5. **Теоремы Геделя о неполноте** (общая форма). *Формальные теории математики удовлетворяют принципам 1.3 и 1.4. Поэтому в достаточно богатых теориях всегда существуют недоказуемые истинные выражения.*

2. НЕПЕРЕЧИСЛИМОСТЬ ИСТИННЫХ ФОРМУЛ

Следующие критерии все являются вариациями на одну тему, хотя это не было очевидным сразу: «аутореферентность, или диагональный процесс» (см. Д и НД).

2.1. Язык S Ar. Мы отсылаем к § 10 гл. II Д и НД за описанием этого языка и его стандартной интерпретации. В § 11 гл. II показано, что множество номеров истинных формул в нумерации Шмульяна неарифметично. Тем более оно неперечислимо, поскольку перечислимые множества даже диофантовы.

2.2. Язык L_1Ar. Здесь мы приведем два варианта аргументов: один дает более сильный результат, а другой — более конкретный. Третий вариант, наиболее близкий к первоначальному рассуждению Геделя, описан в § 5.

а) *Теорема Тарского для* L_1Ar. Мы можем свести доказательство неарифметичности истинных формул в L_1 Ar к теореме Тарского в S Ar следующим способом. Во-первых, множества формул L_1 Ar и S Ar разрешимы во множестве всех выражений (это доказано в § 2 гл. IV для L_1 Ar). Во-вторых, отображение перевода: {формулы S Ar} $\xrightarrow{t_2}$ {формулы L_1 Ar}, описанное в § 10 гл. II книги Д и НД, рекурсивно (это легко установить по образцу рассуждений главы IV). Так как оно сохраняет функции истинности, то $T_s = tr^{-1}(T_{L_1})$ в очевидных обозначениях. Но тогда из арифметичности T_s следовала бы арифметичность (см. доказательство леммы 1.5 гл. IV), что противоречит теореме Тарского для SAr.

Провести это доказательство во всех деталях было бы полезным упражнением для читателя.

Следующее рассуждение проще, точнее, но оно показывает лишь неперечислимость T_{L_1} вместо неарифметичности.

б) Пусть $E \subset Z^+$ — перечислимое, но неразрешемое множество (его существование установлено в § 5 гл. I). Пусть формула $P(x)$ языка L_1 Ar с одной свободной переменной x выражает E. Положим для $n \geqslant 2$: $\bar{n} = (\ldots + (\bar{1} + \bar{1}, \bar{1})\ldots)$, где справа стоит терм — имя целого числа n в очевидной канонической записи типа $\mathscr{L}_1$. Рассмотрим семейство замкнутых формул $\{ \neg (P(\bar{n})) \mid n \in Z^+ \}$ в L_1 Ar.

2.3. Предложение. а) *Отображение* $Z^+ \to \{$*формулы* L_1 Ar$\} : n \to \neg P(\bar{n})$ *рекурсивно.*

б) *Множество* $\{n \mid \neg (P(n))$ *истинна*$\}$ *неперечислимо.*

Следствие. T_{L_1} *неперечислимо; более точно, множество истинных формул семейства* $\{ \neg (P(\bar{n})) \}$ *неперечислимо.* (Иначе прообраз T_{L_1} в Z^+ был бы перечислим.)

Доказательство. а) Пусть формула $\neg (P(x))$ имеет вид соединения $R_1 x \cdot R_2 x \ldots x R_{s+1}$, где x не входит в выражения R_i. В обозначениях доказательства предложения 1.9 гл. IV имеем для фиксированной нумерации N множества выражений с функцией соединения*:

$$N(\neg(P(\bar{n}))) = N(R_1) * N(\bar{n}) * N(R_2) * \ldots * N(R_{s+1}).$$

Поэтому достаточно доказать рекурсивность функции $n \mapsto N(\bar{n})$.

Но так как $\overline{n+1} = +(\overline{1n})$, то при $n \geqslant 1$

$$N(\overline{n+1}) = N(+) * N(\subset) * N(\overline{1}) * N(\overline{n}) * N(\supset),$$

что дает рекурсивное выражение $N(\overline{n+1})$ через $N(\overline{n})$.

б) $\{n \mid \neg(P\ \overline{n})\} \in T_{L_1} = Z^+ \setminus E$

по определению формулы $P(x)$, выражающей E. Но дополнение к E неперечислимо, так как E неразрешимо.

Предложение и следствие доказаны.

2.4. Языки, не менее богатые, чем L_1 Ar. Пусть L — произвольный язык с алфавитом A (конечным или счетным), в котором задано множество «истинных» выражений T. Предположим, что он не беднее языка арифметики в следующем смысле:

Существует отображение перевода

$tr \cdot \{$*формулы* L_1 Ar$\} \to \{$*выражения в* $A\}$, *которое переводит* T_{L_1} *в* T, *дополнение* T_{L_1} *в дополнение к* T, *и рекурсивно.*

Тогда T *неперечислимо.*

Такое отображение можно построить, скажем, для L_1 Set. Предложение 2.3 показывает, что достаточно уметь переводить на языке L даже только формулы из семейства $\neg(P(\overline{n}))$, что позволяет обойтись очень скромным языком арифметики.

2.5. Замечания. а) Серия диофантовых задач «истинна ли $P(\overline{n})$», т. е. «существует ли решение в Z^+ диофантова уравнения $F(n; x_2, \ldots, x_r) = 0$?» ($F$ — подходящий многочлен с целыми коэффициентами)' такова, что для ее полного решения не может хватить никакого финитно описываемого набора доказательных средств.

Можно сказать, что теория диофантовых уравнений уже бесконечно сложна.

б) В некотором смысле любая задача математики сводится к диофантовой. Действительно, переводя ее на подходящий формальный язык, разумно спросить: «доказуема ли формула P или $\neg P$?» Но это есть в точности вопрос о том, попадает ли номер P (номер $\neg P$) в перечислимое множество D доказуемых формул, т. е. о том, разрешимо ли диофантово уравнение из данной серии, отвечающей D.

Это — несколько неожиданное подтверждение мнения Гаусса о королевском статусе арифметики. Существует даже «королевское диофантово уравнение» — проекция графика его есть множество номеров формул в L_1 Set, выводимых из аксиом Цермело — Френкеля.

Конечно, мы привыкли спрашивать «истинна ли P?, а не «доказуема ли P?»

С этой точки зрения высшие творческие акты в математике суть изобретения новых принципов доказательств, которые не редуцируются к «наследию отцов» и должны быть заново принимаемы на веру. Теория множеств в целом была последним таким принципом в ма-

тематике нового времени. Драматическая история ее торжества и неприятия достойна величины этого открытия.

Удивительно, что в рамках формальной математики можно кое-что сказать и о столь неформальных вещах (ср. с. § 5 дальше).

3. О ДЛИНЕ ДОКАЗАТЕЛЬСТВ

3.1 Название этого параграфа воспроизводит заглавие небольшой работы Геделя 1936 года. Содержание его состоит в уточнении и доказательстве следующих качественных утверждений.

Пусть дан формальный язык L вместе с некоторой концепцией выводимости формул P из (переменного) множества формул A. Сверх того, пусть дана некоторая функция, оценивающая «сложность вывода» формулы P из множества $\mathcal{A}$ (это может быть *минимальный объем формального вывода* P из $\mathcal{A}$, т. е. число знаков конечного протоалфавита, входящего в такой вывод). Предположим, что в L заложен определенный фрагмент логики $\mathcal{L}_1$, что L и $\mathcal{A}$ достаточно богаты для действия принципов неполноты и что «сложность вывода» удовлетворяет некоторым естественным аксиомам (не путать ее со сложностью Колмогорова; это совершенно другое понятие).

Тогда справедливы следующие факты:

а) *Существуют выводимые из $\mathcal{A}$ формулы, вывод которых сколь угодно более сложен, чем сама формула.*

Наблюдение показывает, что к этому расплывчатому классу принадлежат если не самые важные, то, по крайней мере, «призовые» математические факты.

б) *Если добавить к аксиомам $\mathcal{A}$ любую независимую формулу A, то найдутся выводимые из $\mathcal{A}$ формулы, вывод которых из $\mathcal{A} \cup \{A\}$ будет сколь угодно проще, чем вывод из $\mathcal{A}$* (принцип ускорения доказательств).

Ср. большую силу «аналитических» методов по сравнению с «элементарными» в теории чисел.

Следующее точное изложение основано на заметке Эренфойхта и Мыцельского в сборнике [6]. В этом сборнике имеются также родственные работы по сложности вычислений и ускорению вычислений.

3.2. Рассмотрим следующий набор данных.

а) *Счетный алфавит* A с фиксированной нумерацией $N : A \to Z^+$.

б) Подмножество $F \subseteq S(A)$, элементы которого называются *формулами*.

в) Частичное отображение $\mathcal{D} : \mathcal{P}(F) \to \mathcal{P}(F)$, которое некоторым множествам формул $\mathcal{A} \subseteq F$ ставит в соответствие множества $\mathcal{D}(\mathcal{A})$ *«выводимых из $\mathcal{A}$»* формул. Вместо $P \in \mathcal{D}(\mathcal{A})$ мы будем писать $\mathcal{A} \vdash P$.

г) *Сложность вывода*: фуикция $\mathrm{Cd}_{\mathcal{A}}(P)$, определенная для пар $\mathcal{A} \subseteq F$, $P \in \mathcal{D}(\mathcal{A})$ и принимающая значения из Z^+. Удобно считать, что $\mathrm{Cd}_{\mathcal{A}}(P) = \infty$, если $P \notin \mathcal{D}(\mathcal{A})$.

Наложим на эти данные следующие условия.

3.3. а) A *содержит* $\neg$, $\rightarrow$, (,).

б) *Если* $P, Q \in F$, *то* $\neg (P)$, $(P) \rightarrow (Q) \in F$. Как обычно, будем писать $P \rightarrow Q$ вместо $(P) \rightarrow (Q)$ и т. п.

$в_1$) $\mathcal{A} \subseteq \mathfrak{D}(\mathcal{A})$; *если* $\mathcal{A} \subset \mathcal{A}'$ *и* $\mathfrak{D}(\mathcal{A})$ *определено, то* $\mathfrak{D}(\mathcal{A}')$ *определено и* $\mathfrak{D}(\mathcal{A}) \subseteq \mathfrak{D}(\mathcal{A}')$.

$в_2$) *Если* $\mathcal{A} \cup \{P\} \vdash Q$, *то* $\mathcal{A} \vdash P \rightarrow Q$.

$в_3$) $\mathcal{A} \vdash P \rightarrow (\neg P \rightarrow Q)$ *для любых* $P, Q \in F$.

$г_0$) *Если* $\mathcal{A} \subseteq \mathcal{A}'$, *то* $\mathrm{Cd}_{\mathcal{A}}(P) \leqslant \mathrm{Cd}_{\mathcal{A}'}(P)$.

$г_1$) *Множество* $\{\langle P, n\rangle \mid \mathrm{Cd}_{\mathcal{A}}(P) \leqslant n\} \leqslant S(A) \times Z^+$ *разрешимо.*

Условие $г_1$) не обязано выполняться для любых $\mathcal{A} \subseteq \mathcal{F}$, но мы будем рассматривать только такие $\mathcal{A}$, для которых оно верно. В случае, когда $\mathrm{Cd}_{\mathcal{A}}(P)$ — объем кратчайшего $\mathcal{L}_1$-вывода P из $\mathcal{A}$ в конечном протоалфавите, а $\mathcal{A}$ — разрешимое множество аксиом, свойство $г_1$) выполняется по следующей причине. Мы можем написать все тексты в A объема $\leqslant n$, которых конечное число, и для каждого из них по очереди проверить, является ли он выводом P из $\mathcal{A}$.

$г_2$) *Существует такая неубывающая по* x *общерекурсивная функция* $l(x, y, z)$, *что*

$$\mathrm{Cd}_{\mathcal{A} \cup \{P\}}(Q) \leqslant l\left(\mathrm{Cd}_{\mathcal{A}}(P \rightarrow Q), N(P), N(Q)\right)$$

для всех $Q \in \mathfrak{D}(\mathcal{A})$.

Обе части неравенства конечны в этих условиях: так как $\mathcal{A} \vdash Q$ в силу $в_1$) имеем $\mathcal{A} \cup \{P\} \vdash Q$, а в силу $в_2$) $\mathcal{A} \vdash P \rightarrow Q$. Оценка типа $г_2$) имеет место в языках $\mathcal{L}_1$, потому что из любого вывода $P \rightarrow Q$ из $\mathcal{A}$ можно получить вывод Q из $\mathcal{A} \cup \{P\}$, просто добавив P, Q (в силу modus ponens). Это увеличивает объем вывода $P \rightarrow Q$ на объемы P и Q.

$г_3$) *Существует такая общерекурсивная функция* $g(x, y)$, что

$$\mathrm{Cd}_{\mathcal{A}}(P \rightarrow (\neg P \rightarrow Q)) \leqslant g(N(P), N(Q)).$$

В языках $\mathcal{L}_1$ формула $P \rightarrow (\neg P \rightarrow Q)$ является логической аксиомой и если $\mathcal{A}$ ее содержит, то вывод аксиомы имеет длину 1 и объем, совпадающий с объемом самой формулы. Последний, конечно, представляется в виде $g(N(P), N(Q))$.

Сформулируем теперь теорему Геделя «об ускорении доказательств». Мы предполагаем, что выполнены соглашения и условия 3.2, 3.3.

3.4. Теорема. а) *Пусть* $\mathcal{A} \subset F$. $\mathfrak{D}(\mathcal{A})$ *неразрешимо. Тогда для любой общерекурсивной функции* l *существует бесконечно много формул* $P \in \mathfrak{D}(\mathcal{A})$, *таких, что*

$$\mathrm{Cd}_{\mathcal{A}}(P) > l(N(P)).$$

б) *Пусть* $\mathcal{A}' = \mathcal{A} \cup \{A\}$ *и формула* A *такова, что* $\mathcal{D}(\mathcal{A} \cap \{\neg A\})$ *неразрешимо. Тогда для любой общерекурсивной функции* r *существует бесконечно много формул* $P \in \mathcal{D}(\mathcal{A})$, *таких что*

$$\mathrm{Cd}_{\mathcal{A}}(P) > r(\mathrm{Cd}_{\mathcal{A}'}(P)).$$

Доказательство. а) Если первое утверждение неверно, то для подходящей l и всех $P \in \mathcal{D}(\mathcal{A})$ имеем $\mathrm{Cd}_{\mathcal{A}}(P) \leqslant l(N(P))$. Но тогда множество

$$\mathcal{D}(\mathcal{A}) = \{P \mid \mathrm{Cd}_{\mathcal{A}}(P) \leqslant l(N(P))\} \subseteq S(A)$$

разрешимо в силу r_1), ибо получается применением ограниченного квантора существования (по n) к разрешимому множеству, описанному в r_1). Это противоречит предложению.

б) Пусть $P \in \mathcal{D}(\mathcal{A} \cup \{\neg A\})$. В силу r_2) имеем

$$\mathrm{Cd}_{\mathcal{A} \cup \{\neg A\}}(P) \leqslant f(\mathrm{Cd}_{\mathcal{A}}(\neg A \to P), N(\neg A), N(P))$$

Если теперь предположить, что второе утверждение теоремы неверно, то для подходящей неубывающей общерекурсивной функции r получим

$$\mathrm{Cd}_{\mathcal{A}}(\neg A \to P) \leqslant r(\mathrm{Cd}_{\mathcal{A}'}(\neg A \to P))$$

или в силу r_2) и r_3)

$$\mathrm{Cd}_{\mathcal{A}}(\neg A \to P) \leqslant r \circ f(\mathrm{Cd}_{\mathcal{A}}(A \to (\neg A \to P)),$$
$$N(A), N(P)) \leqslant r \circ f(g(N(A), N(P)), N(A), N(P)).$$

Подставляя это в самое первое неравенство, получаем при фиксированной A оценку вида

$$\mathrm{Cd}_{\mathcal{A} \cup \{\neg A\}}(P) \leqslant l(N(P)),$$

где l общерекурсивна, $P \in \mathcal{D}(\mathcal{A} \cup \{\neg A\})$. Это противоречит неразрешимости $\mathcal{D}(\mathcal{A} \cup \{\neg A\})$ в силу первого утверждения теоремы.

3.5. **Замечание.** В формулировке теоремы 3.4 существенно условие неразрешимости множества доказуемых формул. Его доказал Черч для любой теории, не менее сильной, чем арифметика.

4. АРИФМЕТИЧЕСКАЯ ИЕРАРХИЯ

4.1 Определим рекурсией по n следующие классы Σ_n, Π_n подмножеств в $(Z^+)^m$ для всевозможных $m = 0, 1, 2\ldots$

а) $\Sigma_0 = \Pi_0 = \{$разрешимые множества$\}$.

б) $\Sigma_{n+1} = \{$проекции коразмерности $\geqslant 1$ элементов $\Pi_n\}$.

в) $\Pi_{n+1} = \{$дополнения к элементам Σ_{n+1} в их объемлющих пространствах$\}$.

Очевидно, Σ_1 — перечислимые множества, Π_1 — дополнения к ним. Следующий результат оправдывает название «арифметической иерархии» для последовательности $\{\Sigma_n, \Pi_n\}$.

4.2. Предложение, а) $\forall n > 0$, $\Sigma_n \cup \Pi_n \subseteq \Sigma_{n+1} \cap \Pi_{n+1}$.

б) $\bigcup_{n=0}^{\infty} \Sigma_n = \bigcup_{n=0}^{\infty} \Pi_n = \{\text{арифметические множества}\}$.

т. е. множества, выразимые формулами языка L_1 Ar.

в) *Множества класса* Σ_n *при* $n \geqslant 1$ *совпадают с множествами, которые выразимы следующими формулами типа* $\mathscr{Q}_1$ *(кванторы — по переменным в* $Z+$, E *— разрешимые множества):*

$\exists x_1 \forall x_2 \exists x_3 \dots \forall x_n \neg (\langle x_1, \dots, x_n, x_{n+1}, \dots, x_m\rangle \in E)$, *n четно;*

$\exists x_1 \forall x_2 \exists x_3 \dots \exists x_n (\langle x_1, \dots, x_n, x_{n+1}, \dots, x_m\rangle \in E)$, *n нечетно;*

аналогично для π_n

$\forall x_1 \exists x_2 \forall x_3 \dots \exists x_n (\langle x_1, \dots, x_n, x_{n+1}, \dots, x_m\rangle \in E)$, *n четно;*

$\forall x_1 \exists x_2 \forall x_3 \dots \forall x_n \neg (\langle x_1, \dots, x_n, x_{n+1}, \dots, x_m\rangle \in E)$, *n нечетно.*

г) *Множества классов* Σ_n, π_n *выразимы аналогичными формулами в* L_1 Ar *со следующими изменениями: вместо* $\langle x_1, \dots, x_n\rangle \in E$ *следует писать любую атомарную формулу; число кванторов перед ней* $\geqslant n$, *но число перемен кванторов (соседних пар вида* $\forall\exists$ *или* $\exists\forall$*) по-прежнему равно* $n - 1$.

Доказательство. а. Проведем индукцию по n. При $n = 0$ имеем $\Sigma_0 \cup \Pi_0 = \Sigma_1 \cap \Pi_1$ по определению разрешимых множеств. Если $\Sigma_{n-1} \subset \Sigma_n$, то $\Sigma_n \subset \Sigma_{n+1}$ (ибо Σ_{n+1} — проекции дополнений к элементам Σ_n, а Σ_n — проекции дополнений к элементам Σ_{n-1}) и $\Pi_n \subset \Pi_{n+1}$ по определению Π. Наконец, $\Pi_n \subset \Sigma_{n+1}$, откуда $\Sigma_n \subset \Pi_{n+1}$: действительно, если $E \in \Pi_n$, то $E \times Z+ \in \Pi_n$ (так как умножение на $Z+$ коммутирует с дополнениями и проекциями и перевозит $\Sigma_0 = \Pi_0$ в себя) и, значит, E — проекция $E \times Z+ \in \Sigma_{n+1}$.

б) Совпадение $\bigcup_{n=0}^{\infty} \Sigma_n = \bigcup_{n=0}^{\infty} \Pi_n$ следует из а). Этот класс множеств содержится в арифметических, ибо перечислимые множества арифметичны, а проекции и дополнения не нарушают арифметичности: им отвечает навешивание $\exists$ и $\neg$.

Для доказательства обратного включения $\{\text{арифметические множества}\} \subseteq \bigcup_{n=0}^{\infty} \Sigma_n = \Sigma_\infty$, заметим, что множества, выразимые атомарными формулами, разрешимы, а остальные получаются из них применением проекций, дополнений, объединений и пересечений (§ 2 гл. II книги Д и НД). Поэтому достаточно проверить, что Σ_∞ замкнут относительно (конечных) пересечений и объединений. Это верно для каждого Σ_n в отдельности. Для Σ_0 это уже было доказано; далее индукция.

Если Σ_n замкнут относительно $\cap$, то Π_n замкнут относительно U, Если $E_1, E_2 \in \Sigma_{n+1}$, E_i — проекция F_i, $F_i \in \Pi_n$, то можно ввести фиктивные переменные и отождествить друг с другом объемлющие F_i пространства и их проекции в пространство, общие для E_i. Тогда $E_1 \cup E_2$ = проекция $F_1 \cup F_2$, так что $E_1 \cup E_2 \in \Sigma_{n+1}$, и значит, Σ_{n+1} замкнут относительно $\cup$.

Наконец, если Σ_n замкнут относительно $\cup$, то Π_n замкнут относительно $\cap$, и аналогичное рассуждение показывает, что Σ_{n+1} замкнут относительно $\cap$.

Здесь, однако, нужно вложить в общее пространство некоторые произведения $F_1 \times (Z+)^{m_1}$, $(Z+)^{m_1} \times F_2$, так, чтобы при отождествлении отображений проекции мы имели

$$\mathrm{pr}\,(F_1 \times (Z^+)^{m_1} \cap (Z^+)^{m_1} \times F_2) = \mathrm{pr}\,F_1 \cap \mathrm{pr}\,F_2.$$

На языке формул это означает, что связанные кванторами $\exists$ переменные в формулах, отвечающих F_1 и F_2, нужно переименовать так, чтобы их множества не пересеклись.

в) Это утверждение получается индукцией по n и прямым применением определений. Связку $\neg$, выражающую дополнение, нужно каждый раз проносить через все кванторы направо, пользуясь обычным правилом коммутирования $\neg\forall = \exists\neg$, $\neg E = \forall\neg$. Проекцию коразмерности $m \geqslant 2$, которая выражается серией кванторов $\exists x_{i1} \ldots x_{i_m}$, нужно сводить к проекции коразмерности 1, заменяя группу переменных $<x_{i_1}, \ldots, x_{i_m}>$ на $<t_1^{(m)}(y), \ldots, t_m^{(m)}(y)>$, меняя соответствующим образом множество E и ставя квантор $\exists y$.

г) Доказательство получается такой же индукцией, как в), с использованием диофантовости множеств из Σ_0. Учесть, что здесь заменять $\exists \ldots \exists$ на $\exists$ же, вообще говоря, нельзя.

Предложение доказано.

4.3. Теорема. *Для всех* $n \geqslant 1$

$$\Sigma_n \setminus \Pi_n \neq \varnothing, \quad \Pi_n \setminus \Sigma_n \neq \varnothing.$$

Доказательство. Утверждение $\Sigma_1 \setminus \Pi_1 \neq \varnothing$ — это теорема 5.8 гл. I о существовании неразрешимых перечислимых множеств. Общий случай доказывается с помощью аналогичного диагонального рассуждения, примененного к версальному семейству.

Пусть $\{E_k\}$ — версальное семейство перечислимых $(n+1)$-множеств над $Z+$, E — его тотальное пространство:

$$\langle k, x_0, \ldots, x_n\rangle \in E \Longleftrightarrow \langle x_0, \ldots, x_n\rangle \in E_k.$$

Положим, считая для определенности $n \equiv 0$ (2):

$$F = \{k \mid \exists x_1 \forall x_2 \ldots \forall x_n \,\overline{\ }\,|\,(\langle k, k, x_1, \ldots, x_n\rangle \in E)\} \subseteq Z^+.$$

В силу 4.2в) $F \in \Sigma_n$. В силу версальности $\{E_k\}$ и 6.2в) любое подмножество $Z+$ из π_n можно выразить в виде

$$F_{k_0} = \{x_0 \mid \overline{\ } (\exists x_1 \forall x_2 \ldots \forall x_n) \,\overline{\ }\,|\,(\langle k_0, x_0, x_1, \ldots, x_n\rangle \in E)\}$$

для подходящего $k_0 \in Z+$. Ясно, что k_0 лежит либо в $F \setminus F_{k_0}$, либо в $F_{k_0} \setminus F$. Поэтому $F \neq F_{k_0}$ и $F \in \Sigma_n \setminus \Pi_n$.

Остальные случаи разбираются аналогично.

4.4. Замечания. а) С точки зрения теорем Тарского и Геделя результаты 4.2 и 4.3 подчеркивают огромное расстояние от доказуемости до истинности: $D \in \Sigma_1$, а T не только не принадлежит Σ_1, но даже выходит за пределы Σ_∞. В следующем параграфе мы укажем некоторые верстовые столбы на этом пути.

б) Формально не оправдана предшествующими рассмотрениями, но имеет смысл классификация арифметических задач, т. е. вопросов «Верно ли, что $P \in T$?», по числу переменных кванторов в замкнутой формуле P, записанной в виде 4.2г).

Как показано в § 1 гл. I книги Д и НД, гипотеза Ферма выражается формулой π_1, а Римана — формулой π_3, хотя есть эквивалентное ей утверждение типа π_1.

Х. Роджерс [2] пишет: «Нетрудно заметить при относительно поверхностном исследовании, что почти все гипотезы, которые (I) интенсивно рассматриваются математиками и (II) выразимы в арифметике, находятся на довольно низком уровне в классификации Σ_n. По-видимому, можно полагать, что человеческий мозг способен понимать и изучать только предложения с не более чем четырьмя-пятью переменами кванторов. Более того, можно считать, что всякие изобретения, подтеории и главные леммы в различных частях математики — это приспособление в помощь мозгу при работе с одной или двумя дополнительными переменами кванторов».

5. ПРОДУКТИВНОСТЬ АРИФМЕТИЧЕСКОЙ ИСТИНЫ

5.1 В этом параграфе мы обсуждаем последний аспект теоремы Геделя: возможность, исходя из любого перечислимого множества уже известных истин арифметики, эффективно пополнить его новыми истинами.

С этой целью рассмотрим первоначальный вариант доказательства, в котором диагональный метод выявлен, а не скрыт в конструкции перечислимого неразрешимого множества. Удобно описать его, сравнив с доказательством теоремы Тарского.

5.2. Пусть задан некоторый язык арифметики (L_1 Ar, SAr или их расширение). Будем считать, что выбрана фиксированная нумерация его алфавита, определяющая фиксированную нумерацию формул N. Для дальнейшего существенно, что конструкция не инварианта относительно замены нумерации на эквивалентную ей.

Как Тарский, так и Гедель опираются на следующую «лемму об автореферентности».

5.3. **Лемма.** *По любой формуле языка с одной свободной переменной $P(x)$ можно эффективно построить замкнутую формулу Q_P, которая говорит: «мой номер не принадлежит множеству, выразимому посредством P».*

Иными словами, Q_P истинная, если и только если $P(\overline{N}(Q_P))$ ложна, где $\overline{N}(Q_P)$ — терм «имя номера Q_P».

Доказательство. Для S Ar эта лемма была установлена в § 11 гл. II книги Д и НД. Для L_1 Ar формула Q_P строится так.

Назовем *диагонализацией* формулы $R(x)$ с одной свободной переменной формулу $R(\overline{N}(R))$. Пусть diag: $Z^+ \to Z^+$ — частичная функция, «N — номер формулы с одной свободной переменной $\mapsto$ N — номер ее диагонализации». Результаты и методы гл. IV позволяют легко установить, что diag вычислима. Поэтому ее график выразим формулой L_1 Ar, которую можно явно построить. Обозначим ее через «y = = diag x», построим формулу $R(x)$: $\exists y$ («y = diag x'' $\wedge$ $P(y)$) и, наконец, положим

$$Q_P : \neg R(\overline{N}(\neg R)) = \text{диагонализация } \neg R.$$

Согласно определениям имеем

Q_P истинна $\Leftrightarrow$ номер $\dashv R$ не удовлетворяет R $\Leftrightarrow$
$\Leftrightarrow$ номер диагонализации $\neg R$ не удовлетворяет P $\Leftrightarrow$
$\Leftrightarrow$ номер Q_P не удовлетворяет P.

Лемма доказана.

Отметим, что проверка выразимости «$y = \mathrm{diag}\ x$» в L_1 Ar требует большой технической работы, из-за чего в книге Д и НД мы и заменили L_1 Ar на S Ar

5.4. Далее рассуждения Тарского и Геделя в параллельном изложении выглядят так:

Тарский:

а) Предположим, что истинность выразима (формулой P)

б) Тогда есть формула, говорящая «я не истинна» (Q_P).

в) Она не может быть ложной (по своей семантике).

г) Она не может быть истинной (по своей семантике).

д) Следовательно, истинность не выразима.

Гедель:

а) Доказуемость выразима (формулой P)

б) Есть формула, говорящая «я не доказуема» (Q).

в) Она не может быть ложной (по своей семантике, иначе она доказуема и потому истинна).

г) Следовательно, она истинна.

д) Следовательно, она же не доказуема (по своей семантике).

Отметим, что пункт в) рассуждения Геделя в нашем пересказе явно использует гипотезу о том, что доказуемы лишь истинные формулы. В 1931 году, когда появилась работа Геделя, специалисты были все еще заняты поисками финитных доказательств непротиворечивости аксиомы арифметики, так что принятие гипотезы $D \subset T$ противоречило бы духу времени Поэтому в редакции самого Геделя рассуждение выглядит несколько иначе. Все это по традиции подробно освещается во всех учебниках логики. Нам достаточно заметить, что если $D \not\subseteq T$, то $D \neq T$ и теорема о неполноте верна тривиально, но мы настолько глубоко заблуждаемся, что это уже и неважно.

Более существенно для нас следующее обстоятельство: по каждой фиксированной концепции доказуемости, приводящей к перечислимому (или даже арифметическому !) множеству доказуемых истинных формул D, можно эффективно построить новую формулу, истинную, но не доказуемую

Уточним, что здесь понимается под «эффективностью».

5.5. **Определение.** *Множество $F \subset Z^+$ называется продуктивным относительно версального семейства 1-множеств $\{E_k\}$, если существует такая частично рекурсивная функция f, что для всех $k \in Z^+$ с $E_k \subset F$ имеем $k \in D(f)$ и $f(k) \in F \setminus E_k$.*

5.6. **Предложение.** *В предложениях п. 7.2 множество (номеров) истинных формул продуктивно относительно версального семейства $\{E_k\}$, построенного в § 8 гл. IV.*

Доказательство. Будем для конкретности работать с языком L_1 Ar. Прежде всего построим перечислимое семейство $\{P_k(x_1)\}$ формул со свободной переменной x_1, таких что P_k выражает E_k. С этой целью определим последовательность термов $\bar{f}[k]$ в L_1 Ar, как в п. 8.1 а), § 8 гл. VI, положив

$\bar{f}[4k] = k = +(\ldots+(\bar{1},\bar{1})\ldots)$, k раз;

$\bar{f}[4k+1] = x_{k+1} = (k+1)$-я переменная L_1 Ar;

$\bar{f}[4k+2] = +(\bar{f}[t_1(k)], \bar{f}[t_2(k)])$;

$\bar{f}[4k+3] = \cdot(\bar{f}[t_1(k)], \bar{f}[t_2(k)])$,

и затем напишем

$$P_k = \exists x_2(\exists x_3 \ldots (\exists x_k(\bar{f}[t_1(k)] = \bar{f}(t_2(k)])\ldots)).$$

Рекурсивность функции $k \to N(P_k)$ легко проверяется методами § 4. После этого, фиксировав перевод «y = diag x», положим

$$R_k = \exists x_{k+1}((''x_{k+1} = \operatorname{diag} x_1'') \wedge (P_k(x_1))),$$

$$Q_{P_k} = {}^{-1}(R_k(\bar{N}({}^{-1}(R_k))))$$

и окончательно

$$f(k) = N(Q_{P_k}).$$

Вычислимость этой функции следует из вычислимости $N(P_k)$. Она удовлетворяет условию 5.5, для T вместо F по лемме 5.3.

5.7. Концепция продуктивности предоставляет следующий подход к задаче исчерпания T: начнем с множества D формул, доказуемых относительно системы аксиом Пеано Ax_0; выразим D_0 формулой P_0; положим $Ax_1 = Ax_0 \cup \{Q_{P_0}\}$; аналогично построим D_1, P_1 и $Ax_2 = Ax_1 \cup \{Qp_1\}$ и т. д. Из теоремы Геделя следует, что пока мы проделываем все это «равномерно эффективно», мы все равно не сможем получить целиком T даже после трансфинитного числа шагов. Тем не менее, как показал С. Феферман, ценой неизбежной утраты эффективности мы можем таким способом получить все T Ar, что́ дает об этом множестве неожиданную и философски интересную информацию.

Сформулируем в заключение результат Фефермана [27].

5.8. Принцип продолжения. Прежде всего для исчерпания TAr недостаточно на каждом шагу добавлять к Ax_i лишь формулу Геделя. Существует много других способов строить интуитивно истинные формулы, по-разному формализуя «веру в аксиомы Ax_i».

Феферман использует, в частности, следующую конструкцию. Пусть система аксиом Ax_α уже построена (α — ординал) и множество номеров выводимых из Ax_α формул выражается формулой D_α. Для любой формулы с одной свободной переменной $P(x)$ построим формулу B^L_α с интуитивным смыслом:

если $P(\bar{n})$ доказуема (исходя из Ax_α) для всех термов-имен чисел $\bar{n}$, то $\forall x\, P(x)$ истинна». Эти формулы должны лежать в T, и мы сможем положить

$$Ax_{\alpha+1} = Ax_\alpha \cup \{B_\alpha^P \mid \text{все } P\},$$

$$Ax_\beta = \bigcup_{\alpha<\beta} Ax_\alpha \text{ для предельных } \beta.$$

Вот способ указать B_α^P явно. Функция $n \to N(P(\bar{n}))$ вычислима как функция от n и $N(P)$. Выразим ее график формулой $M(x, y, z)$ так, что для $d, m, n \in Z^+$

$$M(\bar{l}, \bar{m}, \bar{n}) \text{ истинна} \Leftrightarrow \begin{cases} l \text{ есть номер формул } P \text{ с единственной свободной переменной } x; \\ m \text{ есть номер } P(\bar{n}). \end{cases}$$

После этого положим

$$B_\alpha^P = \forall y \forall z (M(\bar{N}(P), y, z) \to D_\alpha(y)) \to \forall x P(x).$$

5.9. Проблема выбора D_α. Это — наиболее тонкий момент; особенно остро стоит вопрос даже о существовании D_β для предельных ординалов β.

Феферман показывает, как построить D_α для подходящей счетной последовательности ординалов с пределом γ, не превосходящим $\omega_0^{\omega_0^{\omega_0}}$, так, что окажется верным следующий результат.

5.10. Теорема. *Все истинные формулы* L_1 Ar *выводимы из* $U_{\alpha<\gamma} Ax_\alpha$.

Итак, пусть мы приняли аксиомы Пеано.

Тогда для постижения полной истины в арифметике остается еще совершить трансфинитную последовательность актов веры в то, что предшествующие акты веры не были заблуждением.

6. ВЫЧИСЛИМЫЕ ФУНКЦИИ С ОЧЕНЬ БЫСТРЫМ РОСТОМ

6.1. В этом параграфе мы приведем два примера истинных арифметических утверждений, не доказуемых в арифметике, скажем, с аксиомами Пеано. Оба они связаны с существованием очень быстро растущих вычислимых функций: в первом примере по построению, во втором — менее очевидным образом.

6.2. Доказуемо вычислимые функции. Пусть $f: Z^+ \to Z^+$ — некоторая вычислимая (т. е. общерекурсивная) функция. Представим ее график Γ_f в виде диофантова множества. Тогда общерекурсивность f означает истинность утверждения вида

$$\forall x\ \exists!\ y\ \exists x_1\ \ldots . x_N\ (P(x, y; x_1, \ldots, x_N) = 0),$$

где P — многочлен с целыми коэффициентами; кванторы относят к переменным из Z^+.

Среди *истинных* утверждений такого рода некоторые *доказуемы* в данной формальной теории, скажем, в теории Пеано. Но заведомо не все такие истинные утверждения доказуемы. Действительно, множество доказуемых утверждений перечислимо; если n-е доказуемое утверждение определяет вычислимую функцию f_n, то функция $F(n) = f_n(n) + 1$ вычислима, но не содержится в списке доказуемо вычислимых функций. Иными словами, проблема распознавания вычислимых функций среди полувычислимых (заданных своими описаниями) неразрешима.

6.3. Теорема Рамсея. Пусть X — некоторое множество; обозначим через $\mathcal{P}_r(X)$ множество его подмножеств, состоящих из r элементов. Ясно, что если $Y \subset X$, то $\mathcal{P}_r(Y) \subset \mathcal{P}_r(X)$. Подмножество Y называется однородным относительно данного разбиения $\mathcal{P}_r(X)$ на классы, если $\mathcal{P}_r(Y)$ целиком попадает в один класс. Обозначим через $[n]$ множество целых чисел от 1 до n. Теорема Рамсея — это следующее комбинаторное утверждение: *для любых* m, r, $k \geqslant 1$ *существует такое* n, *что для любого разбиения* $\mathcal{P}_r[n]$ *на* k *классов в* $[n]$ *найдется однородное подмножество, содержащее* $\geqslant m$ *элементов*. В частности, с помощью перебора вычислима функция Рамсея $R_0(m, r, k)$, дающая наименьшее значение n с таким свойством

Справедливо также усиление теоремы Рамсея. Чтобы его сформулировать, назовем подмножество $[n]$ *дисперсным*, если количество его элементов не меньше, чем его наименьший элемент

Усиленная теорема Рамсея утверждает, что *для любых* m, r, $k \geqslant 1$ *существует такое* n, *что для любого разбиения* $\mathcal{P}_r[n]$ *на* k *классов в* $[n]$ *найдется дисперсное однородное подмножество, содержащее* $\geqslant m$ *элементов*. Точно так же с помощью перебора вычислима вторая функция Рамсея $R(m, r, k)$, дающая наименьшее значение n с таким свойством.

Оказывается, однако, что хотя теорема Рамсея доказуема в арифметике Пеано, усиленная теорема Рамсея уже не доказуема.

Скорость роста функции R чрезвычайно велика. Уже R_0 растет довольно быстро: $R_0(m, m, m)$ примерно как $2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ (m раз), но $R(m, m, m)$ не поддается никакому воображению. Эти результаты были доказаны Пэрисом и Хэррингтоном [24].

Глава VI

РЕКУРСИВНЫЕ ГРУППЫ

1. ОСНОВНОЙ РЕЗУЛЬТАТ И ЕГО СЛЕДСТВИЯ

1.1. Рассмотрим счетный «групповой алфавит»

$$A = \{a_1, a_2, \ldots; a_1^{-1}, a_2^{-1}, \ldots\}.$$

Выражения в алфавите A, включая пустое выражение Λ, будем по традиции называть *словами*. Слово $a_i \ldots a_i$ ($m \geqslant 1$ раз) будем обозначать a_i^m; $a_i^{-1} \ldots a_i^{-1}$ ($m \geqslant 1$ раз) — соответственно a_i^{-m}; будем считать, что $a_i^0 = \Lambda$. Слово $a_{i_1}^{m_1} \ldots a_{i_k}^{m_k}$ называется *приведенным*, если оно пустое или в его полной записи нет подслов вида $a_i^{-1} a_i$ и $a_i a_i^{-1}$.

На множестве приведенных слов операция «соединение и приведение — вычеркивание всех подслов вида $a_i a^{-1} a_i^{-1} a_i$ определяет структуру группы с единицей Λ, которую мы также будем обозначать 1. Это — свободная группа F со счетным множеством образующих $\{a_1 \ldots, a_n, \ldots\}$. Не обязательно приведенные слова также могут рассматриваться как элементы F: они отождествляются с результатом приведения в F.

На A имеется каноническая нумерация: $N(a_i) = 2i$, $N(a_i^{-1}) = 2i - 1$. Все понятия, связанные с вычислимостью операций и перечислимостью подмножеств в A и $S(A)$ будут рассматриваться по отношению к любой из нумераций A, эквивалентной N, и любой из нумераций $S(A)$, согласованной с N (см. определения в § 1 гл. IV). Мы будем постоянно пользоваться следующими фактами.

1.2. Лемма. а) *Множество F приведенных слов в $S(A)$ разрешимо.*

б) *Групповые операции в F вычислимы.*

в) *Подгруппа $G \subseteq F$ перечислима в $S(A)$ тогда и только тогда, когда у нее есть перечислимое множество образующих.*

г) *Нормальный делитель $H \subseteq G$ в перечислимой подгруппе $G \subseteq F$ перечислим тогда и только тогда, когда он порожден перечислимым множеством как нормальный делитель.*

д) *Гомоформизм $F \to F$ рекурсивен тогда и только тогда, когда рекурсивно индуцированное им отображение*

$$\{a_1, \ldots, a_n, \ldots\} \to F.$$

Это хорошее упражнение на владение техникой гл. IV, и мы оставляем его читателю. Начать доказательство удобно с установления вычислимости операции приведения; все остальное делается более или менее автоматически.

1.3. Определение. *Группа называется рекурсивной, если она изоморфна фактогруппе вида G/H, где $G \subseteq F$ — перечислимая подгруппа, а $H \subseteq G$ — перечислимый нормальный делитель.*

Здесь можно было бы ограничиться подгруппами $G \leqslant F$, которые порождены перечислимым подмножеством стандартных образующих $\{a_1, \ldots, a_n, \ldots\}$.

1.4. **Замечания и примеры.** а) Рекурсивные группы не более чем счетны.

б) Группы, заданные конечным числом образующих и соотношений (*конечно определенные*, сокращенно к.о.), рекурсивны. В частности, рекурсивны конечные группы и *конечно порожденные* (к.п.) абелевы группы.

в) Подгруппа H к.о. группы G не обязана быть к.о. (или даже к.п.) группой. Однако *если она конечно порождена, то она рекурсивна.*

Действительно, пусть $\{h_1, \ldots, h_m\}$ — система образующих H. Дополним ее до системы образующих $\{h_1, \ldots, h_m, h_{m+1}, \ldots, h_n\}$ группы G, где $h_{m+1}, \ldots, h_n$ порождают G и связаны конечным числом соотношений, и определим гомоморфизм $\varphi: F \to G$, $\varphi(a_i) = h_i$ для $i \leqslant n$, $\varphi(a_j) = 1$ для $j > n$. Его ядро E порождено конечным числом соотношений между $h_1, \ldots, h_n$ и множеством $\{a_{n+1}, a_{n+2}, \ldots\}$ и потому перечислимо по лемме 1.2.г). Подгруппа $\overline{H} \subset F$, порожденная $a_1, \ldots, a_m$, также перечислима по лемме 1.2 в). Поэтому множество $\overline{H} \cap E$ перечислимо. Но φ индуцирует изоморфизм $\overline{H}/H \cap E \simeq H$ Следовательно H рекурсивна.

Основная цель этой главы — доказательство следующей замечательной теоремы Хигмэна [28], которая обращает простое утверждение 1.4 в следующую теорему.

1.5. **Теорема.** а) *Любая рекурсивная группа G/H (в обозначениях 1.3) погружается в подходящую к о. группу $F\,N$.*

б) *Это погружение можно считать эффективным, т. е. индуцированным посредством подходящего рекурсивного отображения $G \to F$.*

Вот некоторые ее следствия.

1.6. **Универсальная конечно определенная группа.** *Существует такая к.о. группа U, что любая к.о. группа G может быть погружена в U (значит, и любая рекурсивная группа погружается в U).*

Действительно, любая к.о. группа изоморфна фактору F по нормальному делителю, который порожден конечным множеством приведенных слов в F и всеми a_i для $i \geqslant n$ с подходящим n. Обозначим через $I \subset S(S(A)) \times Z^+$ разрешимое множество пар $\langle$ конечная последовательность приведенных слов, $n\rangle$ и пусть N_t (для $t \in I$) — соответствующий нормальный делитель. Построим «дважды бесконечный» групповой алфавит $\{a_{jk}, a_{jk}^{-1} \mid j, k \geqslant 1\}$, выберем рекурсивную нумерацию множества I, отождествив его с Z^+, и зададим группу U_0 образующими $\{a_{jk}\}$ и соотношениями «N_j, записанными в алфавите $\{a_{j1}, a_{j2}, \ldots\}$». Ясно, что U_0 рекурсивна. Из результатов следующего параграфа будет видно, что U_0 — свободное произведение всех групп F/N_j, поэтому любая к.о. группа в U_0 погружается. Значит, любая

к. о. группа U, в которую по теореме Хигмэна погружается U_n, универсальна.

В работе М. К. Валиева [29] строится универсальная группа U, заданная 14 образующими и 42 соотношениями. Там же указано, что можно ограничится 2 образующими и 27 соотношениями.

1.7. К.о. группа с алгоритмически неразрешимой проблемой тождества слов.

Пусть G — группа с четырьмя свободными образующими a, b, c, d и соотношениями
$b^{-m}ab^m = d^{-m}cd^m$ для всех $m \in E$, где $E \subset Z^+$ — перечислимое неразрешимое множество. Из результатов § 2 легко следует, что в G равенство

$$b^{-x}ab^x = d^{-x}cd^x$$

выполнено *только* для $x \in E$ (В самом деле, элементы $b^{-m}ab^m$ для $m \geqslant 1$ порождают в G свободную подгруппу, так что G содержит свободное произведение подгрупп, порожденных $\{b^{-x}ab^x \mid x \geqslant 1\}$ и $\{d^{-x}cd^x \mid x \geqslant 1\}$ с объединенными подгруппами $\{b^{-x}ab^x = d^{-x}cd^x \mid x \in E\}$. Поэтому справедливость написанного равенства неразрешима (как массовая задача, пронумерованная x), и эффективное погружение G в к.о. группу дает неразрешимость проблемы тождества слов в этой к.о. группе.

Существование таких групп было впервые установлено П. С. Новиковым

1.8. «Естественные» рекурсивные группы. Много примеров рекурсивных групп не являющихся априори конечно определенными, доставляет алгебраическая геометрия над полями алгебраических чисел Ограничимся типичным примером.

Пусть $O_n(Q)$ — группа ортогональных автоморфизмов некоторого n-мерного линейного пространства L (над полем рациональных чисел Q), снабженного квадратичной формой f. Пусть b — соответствующая билинейная форма. Для любого вектора $x \in L$ с $f(x) \neq 0$ определена симметрия $\tau_x \in O(Q)$:

$$\tau_x(y) = y - 2\frac{b(x, y)}{f(x)}x \text{ для всех } y \in L.$$

Инволюции $\tau_x \in O(Q)$ составляют перечислимую систему образующих этой группы, а все соотношения порождены перечислимой (даже разрешимой) системой соотношений
$\tau_x^2 = 1$, $(\tau_x\tau_y\tau_z)^3 = 1$ для всех копланарных $\{x, y, z\}$ (С. Беккен).

Подразумеваемая нумерация $L \cong Q^n$ согласована с любой нумерацией Q, которая Z^+ согласована со стандартной и в которой операции поля вычислимы.

1.9. Теорема Хигмэна родственна теореме о диофантовости перечислимых множеств (гл. II), хотя была впервые доказана раньше последней. Возможно, что оба факта являются частными случаями

подходящего общего утверждения о рекурсивных алгебраических структурах.

Во всяком случае использование теоремы о диофантовости значительно упрощает «рекурсивную» часть доказательства Хигмэна. Это показал М. К. Валиев, рассуждения которого мы приведем в § 5, 6. Теоретико-групповой подготовке посвящены § 2—4; здесь мы следуем Хигмэну.

2. СВОБОДНЫЕ ПРОИЗВЕДЕНИЯ И HNN-РАСШИРЕНИЯ

2.1. Пусть дано семейство групп (G_i), $i \in I$, и семейство гомоморфизмов групп $\alpha_i : A \to G_i$.

Рассмотрим класс семейств (H, β_i) гомоморфизмов $\beta_i : G_i \to H$ с условием: $\beta_i \circ \alpha_i : A \to H$ не зависит от $i \in I$. В этом классе существует единственное с точностью до изоморфизма универсальное семейство $\varphi_i : G_i \to *\limits_A G_k$:, любое другое семейство (H, β_i) однозначно определяется гомоморфизмом $\gamma : *\limits_A G_k \to H$ для которого $\beta_i = \gamma \cdot \varphi_i$.

Ниже мы будем пользоваться только случаем, когда все α_i — вложения. В этом случае $*\limits_A G_k$ называется свободным произведением групп G_i с объединенными подгруппами $\alpha_i(A) \subseteq G_i$. Структурные отображения $G_i \to *\limits_A G_k$ будем обозначать, как правило, φ_i, возможно, с дополнительными индексами. Структурный гомоморфизм $\varphi_i \circ \alpha_i : A \to *\limits_A G_k$, не зависящий от i, обозначим φ.

В случае $A = \{1\}$ мы пишем просто $* G_i$ вместо $*\limits_A G_i$; если множество индексов есть $\{1, \ldots, n\}$, применяется запись $G_1 * \ldots * G_n$ и т. п.

Мы будем постоянно пользоваться следующим структурным результатом.

Пусть $\alpha_i : A \to G_i$ — *вложения* и пусть $S_i \subset G_i$ — такие подмножества, что

$$G_i \setminus \alpha_i(A) = \bigcup_{s \in S_i} \alpha_i(A)\, s \text{ и } \alpha_i(A)\, s_1 \neq \alpha_i(A)\, s_2 \text{ при } s_1 \neq s_2 \in S_i.$$

2.2. Предложение. *Любой элемент группы* $*\limits_A G_i$ *однозначно представляется в виде*

$$\varphi(a)\, \varphi_{i_1}(s_1) \ldots \varphi_{i_n}(s_n),$$

где $a \in A$, $s_k \in S_{i_k}$, $i_j \neq i_{j+1}$ *при всех* j. $n \geqslant 0$, *зависят от элемента.*

Это разложение будем называть каноническим.

Доказательство этого факта и дальнейшие подробности см., например, в лекциях Серра «Деревья, амальгамы и SL_2» (Математика, 18 : 1, 1974, с. 3—51).

2.3. Следствия. а) *В условиях п. 2.3 структурные гомоморфизмы* φ, φ_i *являются вложениями.*

Это позволяет иногда отождествлять A и G_i с подгруппами $*\limits_A G_i$ относительно φ, φ_i. В следующих формулировках мы так и поступим. Однако в многоэтажных конструкциях последующих разделов одна и та же группа будет по-разному вкладываться в другую группу с помощью различных композиций структурных отображений, и за ними придется тщательно следить.

б) $G_i \cap G_j = A$ при $i \neq j$ (в $*\limits_A G_i$), т. е. $\varphi_i(G_i) \cap \varphi_j(G_j) = \varphi(A)$.

Для доказательства включения $\subseteq$ воспользуемся предложением 2.2: иначе мы имели бы $\varphi_i(s_i) = \varphi_j(s_j)$ вопреки единственности.

в) *Пусть дано семейство вложений* $\beta_i : H_i \to G_i$ *и подгруппа* $B \subseteq A$, *такая, что*

$$\beta_i(H_i) \cap \alpha_i(A) = \alpha_i(B) \text{ для всех } i.$$

Тогда композиция $B \xrightarrow{\beta_i^{-1}\cdot\alpha_i} H_i \xrightarrow{\varphi_i\cdot\beta_i} {}_A*G_i$ *не зависит от* i *и потому определено каноническое отображение* ${}_B*H_i \to {}_A*G_i$. *Оно является вложением. В частности, подгруппа* ${}_A*G_i$, *порожденная* $\varphi_i \cdot \beta_i(H_i)$, *изоморфна* ${}_B*H_i$.

Действительно, каноническое разложение элемента ${}_B*H_i$, описанное в п. 2.2, переходит в каноническое разложение его образа в ${}_A*G_i$.

г) *В тех же обозначениях имеем*

$$({}_B*H_i) \cap A = B \text{ в } {}_A*G_i,$$

$$({}_B*H_i) \cap G_j = H_j \text{ в } {}_A*G_i.$$

2.4. Образующие и соотношения. Пусть M — некоторое множество, а R — некоторое подмножество свободной группы F_M, свободно порожденной M. Тогда через $|M : R|$ будем обозначать факторгруппу $F_M/\overline{R}$, где $\overline{R}$ — наименьший нормальный делитель F_M, содержащий R. Это задание группы образующими (M) и соотношениями (R).

Мы будем дополнительно пользоваться следующими вольностями записи.

а) Если M имеет непустое пересечение с какой-то ранее описанной группой, то следствия из соотношений в этой группе подразумеваются входящими в R, даже если они не выписаны. Упоминание об R может вообще быть опущено, если сверх таких соотношений ничего больше нет. Например, если $E, F \subseteq G$ — две подгруппы, то $|E \cup F|$ — порожденная ими подгруппа в G и т. п.

б) В R вместо, скажем, $a_1 a_2^{-1}$ мы можем написать $a_1 = a_2$.

Пример. Если $\alpha_i : A \to G_i$ — вложения, то ${}_A*G_i$ задается образующими и соотношениями так:

$$\left|\bigcup_{i\in I} G_i \mid \alpha_i(a) = \alpha_j(a) \text{ для всех } a \in A_{ij},\ i, j \in I\right|.$$

Введем теперь фундаментальную для всего дальнейшего конструкцию (Г. Хигмэн, Б. Нейманн, Х. Нейманн).

Пусть даны два вложения групп $\alpha, \beta : A \to U$.

2.5 **Определение.** *HNN-расширением группы* G (*относительно* A, α, β) *называется группа*

$$K = |G \cup \{t\} : t^{-1}\alpha(a)t = \beta(a) \text{ для всех } a \in A|.$$

2.6. **Предложение.** *Следующие гомоморфизмы являются вложениями:*

а) $G \to K$, $g \mapsto$ класс $g \in G \bmod$ *соотношений* $\in K$

б) $G *_A t^{-1}Gt \to K$, *где свободное произведение берется относительно вложений* $a \mapsto \beta(a)$, $a \mapsto t^{-1}\alpha(a)t$.

Доказательство. В группе $G * \{u^n\}$ подгруппа U, порожденная G и $u^{-1}\alpha(A)u$, изоморфна $G * u^{-1}\alpha(A)u$. Действительно, каноническое разложение элемента второй группы имеет вид

$$g_1 u^{-1}\alpha(\alpha_1) u g_2 \dots g_n u^{-1}\alpha(\alpha_n) u,$$

где $g_1 \in G$, $g_2, \dots, g_n \in G \setminus \{1\}$;

$a_1, \dots, a_{n-1} \in A \setminus \{1\}$, $a_n \in A$,

и поэтому имеет канонический вид также в $G * \{u^n\}$.

Аналогично построим подгруппу

$$V = G * v\beta(A)v^{-1} \subset G * \{v^n\}.$$

Отождествим с U и V группу $W = G * w^{-1}Aw$ посредством изоморфизмов, тождественных на G и переводящих $w^{-1}aw$, в $u^{-1}\alpha(a)u$, $v\beta(a)v^{-1}$ соответственно.

Рассмотрим группу $(G * \{u^n\}) *_W (G * \{v^n\})$. Группа $G \subset W$ канонически вложена в нее, и элемент $t = uv$ удовлетворяет соотношениям $t^{-1}\alpha(a)t = \beta(a)$ для всех $a \in A$, потому что мы отождествили $u^{-1}\alpha(a)u = v\beta(a)v^{-1}$. Кроме того, из предложения 2.2 видно, что $u^{-1}Gu$, vGv^{-1} порождают в $(G * \{u^n\}) *_W (G * \{v^n\})$ свободное произведение с объединенной подгруппой A, вложенной посредством отображений $a \mapsto u^{-1}\alpha(a)u$, $a \mapsto v\beta(a)v^{-1}$ соответственно. Значит, G и $t^{-1}Gt$ также порождают свободное произведение, описанное в формулировке (применить сопряжение посредством v).

Поэтому подгруппа $K' = \langle G \cup \{t = uv\} \rangle \subseteq (G * \{u^n\}) *_W (G * \{v^n\})$

является гомоморфным образом K, и утверждения а), б) справедливы для K'. Более того, каноническое отображение $K \to K'$ является изоморфизмом. Для проверки достаточно заметить, что существует изоморфизм

$$K * \{v^n\} \simeq (G * \{u^n\}) *_W (G * \{v^n\}),$$

переводящий $t \in K$ в uv.

В частности, порядок t в K бесконечен. Предложение доказано.

Нам понадобится уточнение и обобщение этого результата в двух направлениях. Во-первых, следует рассмотреть итерацию HNN-расширений; во-вторых, связь HNN—расширений группы и подгруппы. Объединим все нужные факты в одной формулировке.

Предположим, что задано целое семейство пар вложений $\alpha_i, \beta_i : A_i \to G$ ($i \in I$) и подгруппа $H \subseteq G$ с условиями $\alpha_i^{-1}(\alpha_i(A) \cap H) = \beta_i^{-1}(\beta_i(A) \cap H) = B_i \subseteq A$ — подгруппы. В этих условиях имеем

2.7. **Предложение.** *Положим*

$$K_G = \langle G \cup \{t_i \mid i \in I\} : t_i^{-1}\alpha_i(a)t_i = \beta_i(a) \text{ для всех } i \in I, a \in A_i \rangle$$

$$K_H = \langle H \cup \{t_i' \mid i \in I\} : t_i^{-1}\alpha_i(b)t_i = \beta_i(b) \text{ для всех } i \in I, b \in B_i \rangle.$$

Тогда

а) *$\{t_i\}$ свободно порождают свободную подгруппу в K_G;*

б) *естественные отображения $G \to K_G$ и $K_H \to K_G : t_i' \mapsto t_i$ являются вложениями. Кроме того, $K_H \cap G = H$ в K_G.*

Доказательство. а) Если бы в K_G из имеющихся соотношений следовало нетривиальное соотношение между t_i, оно сохранилось бы в факторе K_G по наименьшему нормальному делителю, содержащему G. Но в этом факторе соотношения $t_i^{-1}\alpha_i(a)t_i = \beta_i(a)$ превращаются в тривиальные $1 = 1$ и никаких ограничений на образы t_i не накладывают. Это доказывает первую часть.

б) Разберем случай одноэлементного I. В обозначениях доказательства предыдущего пункта рассмотрим K_G как подгруппу $(G * \{u^n\}) * (G * \{v^n\})$. В

$G * \{u^n\}$ имеем по предложению 2.2

$$H * \{u^n\} \cap G * u^{-1}\alpha(A)u = H * u^{-1}\alpha(B)u$$

и аналогично в $G * \{v^n\}$

$$H * \{v^n\} \cap G * v\beta(A)v^{-1} = H * v\beta(B)v^{-1}.$$

Описанное выше отождествление U с V отождествляет эти пересечения с подгруппой

$$W_0 = H * w^{-1}Bw \subseteq G * w^{-1}Aw = W.$$

Из следствия 2.3в) находим каноническое вложение

$$(H * \{u^n\}) *_{W_0} (H * \{v^n\}) \to (G * \{u^n\}) *_{W} (G * \{v^n\}).$$

Но, как в конце доказательства 2.6, группа слева есть $K_H * \{v^n\}$, а справа — $K_G * \{v^n\}$, что дает вложение $K_H \to K_G$.

Далее (пересечение в $(G * \{u^n\}) *_W (G * \{v^n\})$):

$$(H * \{u^n\}) *_{W^0} (H * \{v^n\}) \cap G * v^{-1}\alpha(A)u = H * u^{-1}\alpha(B)u,$$

откуда, пересекая еще с G, получаем H. Тем более, $K_H \cap G = H$.

Отсюда случай общего I получается для конечных I несложной индукцией по n, а для бесконечных — переходом к индуктивному пределу (здесь — объединению). Подробности мы оставляем читателю.

3. ВЛОЖЕНИЯ В ГРУППЫ С ДВУМЯ ОБРАЗУЮЩИМИ

В этом параграфе мы докажем результат, который будет использован в дальнейшем и в то же время выпукло продемонстрирует в простой ситуации приемы уменьшения числа образующих при вложении.

3.1. Предложение. а) *Любую счетную или конечную группу можно вложить в группу с двумя образующими.*

б) *Если G рекурсивна, то вложение можно сделать рекурсивным.*

Доказательство. а) В $Z * Z = \{b^n\} * \{v^n\}$ есть свободная подгруппа счетного ранга, например:

$$S = |\{b^{-i}vb^i \mid i > 0\}|.$$

Отсутствие соотношений между образующими $b^{-i}vb^i$ немедленно следует из предложения 2.2.

Поэтому если G — свободная счетная группа, то она погружается в $Z * Z$. В противном случае можно попытаться представить G в виде F/N, где F счетна

и свободна, погрузить F в $Z * Z$ и затем рассмотреть индуцированный гомоморфизм $F/N \to Z * Z/N'$, где N' — нормальный делитель в $Z * Z$, порожденный N. К сожалению, $N' \cap F$ может быть строго больше N, так что этот гомоморфизм не обязан быть вложением. Следующая конструкция показывает, как с этим бороться.

Пусть $\{g_1, g_2, g_3, \ldots\}$ — счетная система образующих группы G, $g_i \neq 1$. Последовательно построим следующие расширения группы G:

1) $G * \{u^n\}$.

2) HNN-расширение группы $G * \{u^n\}$:

$$|G * \{u^n\} \cup \{t_i \mid t_i^{-1} u t_i = u g_i,\ i = 1, 2, \ldots\}|.$$

Учесть, что u, ug_i порождает в $G * \{u^n\}$ бесконечные циклические подгруппы.

3) Свободное произведение P этого HNN-расширения и группы $\{b^n\} * \{v^n\}$ с объединенными подгруппами $|\{t_1, t_2, \ldots\}|$, $|\{b^{-i} v b^i \mid i \geqslant 1\}|$ относительно изоморфизма

$$t_i = b^{-i} v b^i,\ i \geqslant 1.$$

4) В P есть две свободные подгруппы ранга 2: $|\{b, v\}|$ и $|\{u, b\}|$. Отсутствие соотношений между u, b следует из того, что они не могут появиться в факторе по минимальному нормальному делителю, содержащему G, t_i, v.

Окончательно построим HNN-расширение группы P:

$$Q = |P \cup \{a\} : a^{-1} b a = u,\ a^{-1} v a = b|.$$

Для завершения доказательства осталось проверить, что Q *порождена элементами* a, b.

Действительно, очевидную систему образующих Q составляет множество $\{g_i,\ t_i\ (i \geqslant 1);\ u,\ v,\ a,\ b\}$.

Соотношения $g_i = u^{-1} t_i^{-1} u t_i$ позволяют исключить g_i.

Соотношения $t_i = b^{-i} v b_i$ позволяют исключить t_i.

Соотношения $u = a^{-1} b a$, $v = a b a^{-1}$ позволяют исключить u, v. Это доказывает первую часть предложения. Следующий анализ конструкции устанавливает вторую часть.

Выражая g_i через a, b в Q с помощью выписанных соотношений, находим $g_i = e_i \bmod$ соотношений в Q, где $e_i = a^{-1} b^{-1} a b^{-i} a b^{-1} a^{-1} b^i a^{-1} \times$ $\times b a b^{-2} a b a^{-1} b^2$. Поэтому в группе $\{a^n\} * \{b^n\}$ подгруппа $|\{e_i \mid i \geqslant 1\}| = E$ обладает следующим замечательным свойством: любой нормальный делитель $N \leqslant E$ порождает в $\{a^n\} * \{b^n\}$ такой нормальный делитель N', что $E \cap N' = N$ (ср с обсуждением в начале доказательства).

В частности, если $\{g_i\}$ — перечислимая система образующих группы G, связанная перечислимым множеством соотношений, то отображение $g_i \mapsto e_i \bmod$ соотношений порождает рекурсивное вложение G в рекурсивную группу E/N', ибо N' перечислимо вместе с N.

4. ХОРОШИЕ ПОДГРУППЫ

4.1 Определение-лемма. *Пусть G — конечно порожденная группа, $H \subseteq G$ — ее подгруппа. H называется хорошей, если выполнены следующие условия:*

а) *Существует конечно определенная группа K, ее конечно порожденная подгруппа L и вложение $G \subset K$, такое, что $G \cap L = H$.*

б) *HNN-расширение*

$K_G = |G \cup \{t\} : t^{-1} h t = h$ *для всех* $h \in H|$ *вкладывается в конечно определенную группу.*

в) $G *_H G$ *вкладывается в конечно определенную группу.*

Доказательство эквивалентности. а)⇒ б). Пусть $G \subset K$, L удовлетворяют а). Тогда K_G вкладывается в HNN-расширение $\langle K \cup \{t\} : t^{-1}lt = l$ для всех $l \in L\rangle$ в силу 2.6. Оно конечно определено: к образующим K нужно добавить t, а к соотношениям между образующими K — соотношения $t^{-1}l_i t = l_i$ для конечной системы образующих $\{l_i\}$ группы L.

б) ⇒ в). Группа $G *_H G$ вкладывается в K_G в силу 2.6б), а K_G вкладывается в к. о. группу по предложению б).

в) ⇒ а). Пусть $G *_H G \subset M$, M конечно определена. Тогда положим $K = M$, $L =$ образ G при сквозном вложении $\varphi_2 : G \to G *_H G \to M$ и вложим G в K посредством $\varphi_1 : G \to G *_H G \to M$. Из того, что $\varphi_1(G) \cap \varphi_2(G) = H$, следует требуемое.

Основная цель этого параграфа состоит в сведении теоремы 1.5 Хигмэна к доказательству того, что перечислимые подгруппы в $Z * Z$ хороши. Для этого и для дальнейших нужд нам понадобится следующая лемма.

4.2. Лемма. *Пусть R — хорошая подгруппа к. п. свободной подгруппы F, $\overline{R}$ — порожденный ею нормальный делитель. Тогда $F/\overline{R}$ можно вложить в к. о. группу.*

Доказательство. Пусть ι — вложение F_R F в к. о. группу K (см. 4.1в)) и пусть $\varphi_1, \varphi_2 : F \to F *_R F$ — структурные отображения. Рассмотрим два вложения F в $K \times F/\overline{R}$:

$$\alpha : f \mapsto \langle \iota \circ \varphi_1(f),\ f\overline{R}\rangle,$$

$$\beta : f \mapsto \langle \iota \circ \varphi_2(f),\ 1\rangle.$$

На подгруппе $R \subset F$ они, очевидно, совпадают. Поэтому они индуцированы гомоморфизмом

$$\gamma : F *_R F \to K \times F/\overline{R},$$

который имеет тривиальное ядро (это так для композиции γ с проекцией на K, совпадающей с ι).

Построим HNN-расширение, переводящее $\iota \times \{1\} : F *_R F \to K \times F/\overline{R}$ в γ:

$$L = \langle K \times F/\overline{R} \cup \{t\} : t^{-1}\langle \iota \circ \varphi_1(f),\ 1\rangle t = \langle \iota \circ \varphi_1(f),\ f\overline{R}\rangle,$$
$$t^{-1}\langle \iota \circ \varphi_2(f),\ 1\rangle t = \langle \iota \circ \varphi_2(f),\ 1\rangle \text{ для всех } f \in F\rangle.$$

Очевидно, L содержит $\overline{F}/R$. Покажем, что она конечно определена.

Образующие L : $\{t\} \cup \{$*отмеченные образующие* $K\} \cup \{$*отмеченные образующие* $F\}$. Эта система конечна.

Соотношения в L: а) {соотношения между образующими K};

б) {соотношения коммутирования между образующими K и образующими F}.

Наложив их, мы можем считать, что дальше работаем в $K \times F$.

в)

$$t^{-1}\langle \iota \circ \varphi_1(f),\ 1\rangle t = \langle \iota \circ \varphi_1(f),\ f\rangle,$$

$$t^{-1}\langle \iota \circ \varphi_2(f),\ 1\rangle t = \langle \iota \circ \varphi_2(f),\ 1\rangle,$$

где f пробегает отмеченные образующие F.

г) Соотношения между образующими F, принадлежащие R.

Систему соотношений $R_0 = a) \cup б) \cup в)$ можно взять конечной. Остается только проверить, что г) следует из нее.

Пусть $R' \subset F$ — нормальный делитель, порожденный R_0, т. е. ядро естественного гомоморфизма $F \to |K \cup F \cup \{t\} : R_0|$. Мы хотим установить, что $R' = \overline{R}$. Включение $R' \subseteq \overline{R}$ очевидно. Проверим обратное включение.

Для $f \in F$ положим $f' = f \bmod R'$, $f_{1,2} = i \quad \varphi_{1,2}(f) \in K$. Тогда из соотношений б) и в) следует, что в $K \times F/R'$ имеем

$$t^{-1} <f_1, 1> t = <f_1, 1> <1, f'>,$$
$$t^{-1} <f_2, 1> t = <f_2, 1>.$$

С другой стороны, если $f \in R$, то, поскольку $F_R * F$ вложена в K из соотношений а) следует, что $f_1 = f_2$. Поэтому $f' = 1$, так что $R \subseteq R'$.

Выведем из этой леммы редукционный результат.

4.3. Предложение. *Если все перечислимые подгруппы в $Z * Z$ хороши, то теорема Хигмэна верна.*

Доказательство. Пусть G — свободная группа, порожденная перечислимым множеством свободных образующих $\{g_i\}$, $i = 1, 2, 3, \ldots$, $N \subset G$ — ее перечислимый нормальный делитель. Покажем, как вложить G/N в к. о. группу.

Рассмотрим сначала вложение $G \to \{a^n\} * \{b^n\}$, $g_i \mapsto l_i$, где l_i описаны в конце § 3. Пусть при этом вложении N порождает нормальный делитель $N' \subset \{a^n\} * \{b^n\}$. По замечанию в конце § 3 G/N вкладывается в $\{a^n\} * \{b^n\}/N'$. Но N' перечислим по лемме 1.2 г), ибо порожден образом перечислимого множества при рекурсивном отображении. Значит, N' — хороший нормальный делитель. Лемма 4.2 показывает тогда, что $\{a^n\} * \{b^n\}/N'$ можно вложить в к. о. группу.

В заключение этого параграфа установим несколько полезных свойств хороших подгрупп.

4.4. Лемма. *Пусть E, $F \subseteq G$ — хорошие подгруппы. Тогда*

а) *$E \cap F$ — хорошая подгруппа;*

б) *$|E \cup F|$ («сумма E и F в G») — хорошая подгруппа.*

Доказательство. а) Пусть φ_1, $\varphi_2 : G \to G *_E G$ и φ_1', $\varphi_2' : G \to G *_F G$ — структурные гомоморфизмы. Пусть M_1, M_2 — такие к. о. группы, что $G *_E G \subseteq M_1$ и $G *_F G \subseteq M_2$. Отождествим $\varphi_1(G) \subseteq M_1$ и $\varphi_1'(G) \subseteq M_2$ с G и построим группу $M_1 *_G M_2$. Она конечно определена (к соотношениям в M_1 и M_2 достаточно добавить соотношения $\varphi_1(g_i) = \varphi_1'(g_i)$ для конечной системы образующих G). Пусть $\varphi_1'', \varphi_2'' : M_1, M_2 \to M_1 *_G M_2$ — структурные вложения. Положим $K = M_1 *_G M_2$, $L = \varphi_1'' \circ \varphi_2(G)$ и вложим G в K посредством $\varphi_2' \circ \varphi_2'$.

Утверждается, что $G \cap L = E \cap F$ (как подгруппа G в K). Действительно, $\varphi_1''(M_1) \cap \varphi_2''(M_2) = G$ с каноническим вложением в $M_1 *_G M_2$. Если в M_1 взять лишь $\varphi_2(G)$, а в M_2 лишь $\varphi_2'(G)$, то пересечение с объединенной подгруппой G даст E и F соответственно, а друг с другом $E \cap F$.

б) Подгруппы $\varphi_1(|E \cup F|)$ и $\varphi_2(G)$ в $G *_E G$ имеют одинаковое пересечение с объединенной подгруппой: они ее содержат. Поэтому в силу 2.3г) в $G *_E G$ имеем

$$\varphi_1(|E \cup F|) \cup \varphi_2(G)| \cap \varphi_1(G) = |E \cup F|,$$

т. е. поскольку E объединена,

$$|\varphi_1(F) \cup \varphi_2(G)| \cap \varphi_1(G) = |E \cup F|.$$

Аналогично

$$|\varphi_1'(E) \cup \varphi_2'(G)| \cap \varphi_1'(G) = |E \cup F|.$$

Обозначения согласованы с тем, что эти пересечения отождествляются в объединенной подгруппе произведения $M_1 *_G M_2$, построенного, как в пункте а).

Применяя 2.3г) к этому произведению, находим

$$|\varphi_1''(|\varphi_1(F) \cup \varphi_2(G)|) \cup \varphi_2''(|\varphi_1'(E) \cup \varphi_2'(G)|) \cap G = |E| \cup F|.$$

Но группа $|\varphi_1'' \circ \varphi_2(G) \cup \varphi_2'' \circ \varphi_2'(G)| \cap G$, очевидно, содержит правую часть этого равенства и содержится в левой, поэтому она также совпадает с $|E \cup F|$.

Наконец, $|\varphi_1'' \circ \varphi_2(G) \cup \varphi_2'' \circ \varphi_2'(G)|$ конечно порождена в к. о. группе $M_1 *_G M_2$, что завершает доказательство.

4.5. Лемма. *Пусть G, H — к. п. подгруппы к. о. групп. Тогда любой гомоморфизм G в H переводит хорошие подгруппы G в хорошие подгруппы H.*

Доказательство. а) Если $A \subseteq G$ хорошая, то $A \times \{1\} \subseteq G \times H$ — тоже хорошая: по вложению (G, A) в (K, L) условиями 4.1 а) строится очевидное вложение $(G \times H, A \times \{1\})$ в $(K \times M, L)$, которое также удовлетворяет 4.1а), если M — к. о. группа, содержащая H.

Наоборот, если $A \times \{1\} \subseteq G \times H$ хорошая, то по вложению 4.1а) $(G \times H, A \times \{1\})$ в (K, L) строится соответствующее вложение (G, A) в $(K, L \cap G \times \{1\})$.

б) Пусть теперь $\varphi\colon G \to H$ — любой гомоморфизм, F — его график $\{A \subseteq G$ — хорошая подгруппа. Тогда имеем в $G \times H$

$$\{1\} \times \varphi(A) = |(|A \times \{1\} \cup \{1\} \times H| \cap F) \cup G \times \{1\}| \cap \{1\} \times H.$$

Из предположений относительно G, H ясно, что F — хорошая подгруппа в $G \times H$. Из пункта а) видно, что остальные подгруппы в правой части формулы тоже хорошие. По лемме 3.2 $\{1\} \times \varphi(A)$ — хорошая подгруппа. Поэтому и $\varphi(A)$ хорошая.

5. ОГРАНИЧЕННЫЕ СИСТЕМЫ ОБРАЗУЮЩИХ

5.1. Пусть $G' = |\{a_0, \ldots, a_n\}|$, $n \geqslant 1$ — группа, свободно порожденная образующими a_i. Назовем подмножество $R' \subset G'$ *ограниченным*, если существует такое $r \geqslant 1$, что любой элемент R' может быть представлен в виде $a_{i_1}^{\varkappa_1} \ldots a_{i_r}^{\varkappa_r}$, $\varkappa_i \in Z$.

В этом параграфе мы докажем следующий частный случай посылки предложения 4.3.

5.2. Предложение. *Если подгруппа $H' \subseteq G'$ порождена ограниченным перечислимым подмножеством $R' \subset G'$, то она хороша.*

Следствие. *То же верно для G', являющихся к. п. подгруппами к. о. групп* (воспользоваться леммой 4.5).

В следующем параграфе будет показано, как общий случай выводится из этого.

Доказательство 5.2. состоит из очередной серии редукционных шагов.

5.3. Первая редукция. Рассмотрим в свободной группе

$$G = |\{a_0, b_0, c_0; \ldots; a_{rn}, b_{rn}, c_{rn}\}|$$

и екоторое множество «слоеных» слов вида

$$R = \left\{ a_0^{x_0} b_0 c_0^{x_0} \dots a_{rn}^{x_{rn}} b_{rn} c_{rn}^{x_{rn}} \right\}$$

и порожденную им подгруппу $H \subseteq G$. Мы покажем в дальнейшем, что *если R перечислимо, то H хороша*. Это — частный случай 5.2, к которому общая ситуация сводится следующим приемом.

Пусть даны G', R', как в п. 5.1. По каждому элементу $g' = a_{i_1}^{x_1} \dots a_{i_r}^{x_r} \in R'$ построим элемент $g \in G$ следующим образом. Представим g' в виде

$$\prod_{i=1}^{n} a_i^{x_{1,i}} \prod_{i=1}^{n} a_i^{x_{2,i}} \dots \prod_{i=1}^{a} a_i^{x_{r,i}},$$

где

$$x_{k,i} = \begin{cases} x_k & \text{при } i = i_k, \\ 0 & \text{при } i \neq i_k. \end{cases}$$

После этого положим

$$g = \left(\prod_{i=1}^{n} a_i^{x_{1,i}} b_i c_i^{x_{1,i}} \right) \dots \left(\prod_{i=1}^{n} a_i^{x_{r,i}} b_i c_i^{x_{r,i}} \right).$$

Если R' перечислимо, то множество R всех элементов g, полученных так из всевозможных $g' \in R'$, перечислимо.

Рассмотрим сюръективный гомоморфизм φ: $G \to G'$: $\varphi(a_i) = a_i$, $\varphi(b_i) = \varphi(c_i) = 1$ для всех $i = 0, \dots, n$. Ясно, что $\varphi(R) = R'$ и, значит, $\varphi(H) = H'$. Из леммы 4.5 тогда следует, что если R хороша в G, то R' хороша в G'.

5.4. Использование диофантовости перечислимых множеств.

Начиная с этого места, мы фиксируем пару (G, перечислимое R), как в п. 5.3. Вместо rn будем писать $l \geqslant 1$ и определим множество $E \subseteq Z^{l+1}$ условием

$$R = \left\{ a_0^{x_0} b_0 c_0^{x_0} \dots a_l^{x_l} b_l c_l^{x_l} \,\middle|\, \langle x_0, \dots, x_l \rangle \in E \right\}.$$

Нетрудно убедиться, что перечислимость R равносильна перечислимости E.

Мы покажем сейчас, что *E можно представить в виде проекции на первые $l+1$ координат множества*

$$\bigcap_{s=1}^{N} E_s \subset (Z)^{l+1} \times (Z)^{m-l}, \quad m \geqslant l+2,$$

где каждое из E_s задается одним из уравнений вида

$x_i = c$, $c \in Z$;

$x_l = x_j$, $0 \leqslant i, j \leqslant m$

или

$x_k = x_j + x_i$,

$x_k = x_j \cdot x_i$, где $l+1 \leqslant k < j < i \leqslant m$.

В самом деле, пусть $\mathscr{E}_0, \ldots, \mathscr{E}_e \in \{1, -1\}$, $\overline{\mathscr{E}} = \langle \mathscr{E}_0, \ldots, \mathscr{E}_l \rangle$. Рассмотрим перечислимые множества

$$E^{\overline{\mathscr{E}}} = \{\langle x_0, \ldots, x_l \rangle \in (Z^+ \cup \{0\})^{l+1} \mid \langle \mathscr{E}_0 x_0, \ldots, \mathscr{E}_l x_l \rangle \in E\}.$$

По основной теореме гл. VI существуют такие многочлены с целыми коэффициентами $P^{\overline{\mathscr{E}}}$, что

$E^{\overline{\mathscr{E}}}$ = проекция 0-уровня $P^{\overline{\mathscr{E}}}$ в $(Z^+ \cup \{0\})^{l+1} \times (Z^+)^{n-l}$ на первые $l+1$ координат $\langle x_0, \ldots, x_l \rangle$. При этом можно считать n настолько большим, что множества «пропадающих» при проекции переменных, реально входящих в $P^{\overline{\mathscr{E}}'}$ и $P^{\overline{\mathscr{E}}''}$, при $\overline{\mathscr{E}}' \neq \overline{\mathscr{E}}''$ не пересекаются. Добавив к пропадающим при проекции переменным еще $(n+1)2^{l+3}$ новых переменных $y_{ij\overline{\mathscr{E}}}$ $(0 \leqslant i \leqslant n,\ j = 1, 2, 3, 4)$, мы получим, что E можно представить в виде проекции на первые $l+1$ координат 0-уровня многочлена

$$Q = \prod_{\overline{\mathscr{E}}} \left(\left(P^{\overline{\mathscr{E}}} (\mathscr{E}_0 x_0, \ldots, \mathscr{E}_l x_l, x_{l+1}, \ldots, x_n) \right)^2 + \sum_{i=0}^{l} \left(\mathscr{E}_i x_i - \sum_{j=1}^{4} y_{ij\overline{\mathscr{E}}}^2 \right)^2 + \right.$$

$$\left. + \sum_{i=l+1}^{n} \left(x_i - 1 - \sum_{j=1}^{4} y_{ij\overline{\mathscr{E}}}^2 \right)^2 \right)$$

уже в $Z^{l+1} \times (Z)^{n+(n+1)2^{l+3}-l}$.

Наконец, чтобы представить множество $Q = 0$ в виде проекции пересечения $\bigcap_{s=1}^{N} E_s$ описанного выше вида, будем вводить дополнительные переменные следующим способом. Пусть $x_0, \ldots, x_t$ — переменные, входящие в Q. Вместо $Q = 0$ напишем $Q_1 = Q_2$, где Q_1 — сумма одночленов Q с положительными коэффициентами, а Q_2 — с отрицательными. Тогда 0-уровень Q = проекция $(x_{t+1} = Q_1) \cap \cap (x_{t+2} = Q_2) \cap (x_{t+1} = x_{t+2})$. Если Q_1 и Q_2 суть константы или переменные, искомое представление найдено. Иначе, скажем, Q_1 можно представить в виде $Q_1' + Q_1''$ либо $Q_1' \cdot Q_1'$ и написать, введя дополнительные переменные:

$$(x_{t+1} = Q_1' + Q_1'') = \text{проекция } (x_{t+3} = Q_1') \cap (x_{t+4} = Q_1'') \cap (x_{t+1} = x_{t+3} + x_{t+4}).$$

Индукция по сумме коэффициентов и степени Q даст требуемое.

5.5. **Вторая редукция.** Теперь мы считаем, что для пары G, R, описанной в п. 5.3, зафиксировано представление E в виде проекции $\bigcap_{s=1}^{N} E_s$ вида, описанного в п. 5.4. В этом пункте мы покажем, что подгруппа $H \subseteq G$, порожденная R, хороша, если хороши все подгруппы

$H_s \subseteq G$, $s = 1, \ldots, N$

описываемые следующим образом:

$$\overline{G} = \left| \{a_0, b_0, c_0; \ldots; a_m, b_m, c_m; \bar{a}_1, \bar{b}_1, \bar{c}_1, \ldots, \bar{a}_l, \bar{b}_l, \bar{c}_l\} \right|,$$

$$\overline{H}_s = \left| \left\{ \left(\prod_{i=l+1}^{m} a_i^{x_i} b_i c_i^{x_i} \right)^{-1} \left(\prod_{i=1}^{l} \bar{a}_i^{x_i} \bar{b}_i \bar{c}_i^{x_i} \right)^{-1} \prod_{i=0}^{m} a_i^{x_i} b_i c_i^{x_i};\ \langle x_0, \ldots, x_m \rangle \in E_s \right\} \right|.$$

С этой целью положим

$$a(x_0, \ldots, x_m) = \left(\prod_{i=l+1}^{m} a_i^{x_i} b_i c_i^{x_i} \right)^{-1} \left(\prod_{i=1}^{l} \bar{a}_i^{x_i} \bar{b}_i \bar{c}_i^{x_i} \right)^{-1} \prod_{i=0}^{m} a_i^{x_i} b_i c_i^{x_i}. \qquad (1)$$

Множество слов $\{a(x_0, \ldots, x_m); \langle x_0, \ldots, x_m \rangle \in Z^{m+1}\}$ свободно: **действительно**, при соединении пары таких слов (или одного слова и обратного к другому такому слову) взаимное сокращение не может загронуть «середины» каждого слова, состоящей из символов $\bar{a}_i$, $\bar{b}_i$, $\bar{c}_i$.

Отсюда следует, что

$$\bigcap_{s=1}^{N} \bar{H}_s = \left| \left\{ a(x_0, \ldots, x_m). \langle x_0, \ldots, x_m \rangle \in \bigcap_{s=1}^{N} E_s \right\} \right|$$

и подгруппа $\bar{H} = \bigcap_{s=1}^{N} \bar{H}_s \subseteq \bar{G}$ хороша, если все $\bar{H}_s$ хороши. Наконец,

$$|\bar{H} \cup \{a_{l+1}, b_{l+1}, c_{l+1}, \ldots, a_m, b_m, c_m; \bar{a}_1, \bar{b}_1, \bar{c}_1, \ldots, \bar{a}_l, \bar{b}_l, \bar{c}_l\}| =$$

$$= \left| \left\{ \prod_{i=0}^{l} a_i^{x_i} b_i c_i^{x_i}, \langle x_0, \ldots, x_l \rangle \in E = \text{проекция} \bigcap_{i=1}^{N} E_s \right\} \cup \{a_{l+1}, b_{l+1}, c_{l+1}, \ldots \right.$$

$$\left. \ldots, \bar{a}_l, \bar{b}_l, \bar{c}_l\} \right|,$$

откуда

$$H = |\bar{H} \cup \{a_{l+1}, b_{l+1}, \ldots, \bar{b}_l, \bar{c}_l\}| \cap |\{a_0, \ldots, b_l, c_l\}|$$

и эта подгруппа хороша вместе с $\bar{H}$.

5.6. Конструкция группы K. Мы будем проверять, что $\bar{H}_s \subseteq \bar{G}$ — хорошие подгруппы, пользуясь критерием 4.1а): явно построим конечно определенную группу $K \supseteq \bar{G}$ и конечно порожденные подгруппы $L_s \subseteq K$, такие, что $L_s \cap \bar{G} = \bar{H}_s$ для всех $s = 1, \ldots, N$.

Группа K будет построена как кратное HNN-расширение $\bar{G}$.

а) *Первое HNN-расширение.* Положим

$$K_0 = |\bar{G} \cup \{t_0, \ldots, t_m\} : R_0|,$$

где R_0 — множество соотношений вида

$$\begin{cases} t_i^{-1} b_i t_i = a_i b_i c_i, \quad i = 0, \ldots, m; \\ t_i^{-1} \bar{b}_i t_i = \bar{a}_i \bar{b}_i \bar{c}_i; \\ t_i \text{ коммутируют со всеми остальными образующими } \bar{G}. \end{cases} \qquad (2)$$

б) Второе HNN-расширение. Положим

$$K = |K_0 \cup \{t_{ijk};\ l+1 < k < i,\ k < j,\ i \neq j;\ i, j, k \leqslant m\} : R|,$$

где R — множество соотношений вида

$$\begin{cases} t_{ijk}^{-1} b_i t_{ijk} = a_i b_i c_i, \\ t_{ijk}^{-1} c_j t_{ij} = t_k c_j, \\ t_{ijk} \text{ коммутирует с } t_k \text{ и остальными образующими } \bar{G}. \end{cases} \qquad (3)$$

В отличие от 5.6а) не вполне очевидно, что K есть HNN-расширение K_0. Для проверки этого достаточно установить, что отображение φ_{ijk} множества {образующие $\overline{G}$} $\cup$ $\{t_k\}$ в себя (i, j, k фиксированы; $i \neq k$, $j \neq k$):

$$\begin{cases} b_l \to a_i\, b_l\, c_i, \\ c_j \to t_k\, c_j, \\ t_k \to t_k, \end{cases}$$

тождественное на остальных образующих G, продолжается до некоторого автоморфизма подгруппы $|\overline{G} \cup \{t_k\}| \subseteq K_0$. Имеем

$$\left|\overline{G} \cup \{t_k\}\right| = \left|\overline{G}_* \left\{t_k^n\right\} : t_k^{-1}\, b_l\, t_k = b_l;\ t_k^{-1}\, a_j\, t_k = a_j;\ \ldots\right|,$$

где многоточие заменяет соотношения, не зависящие от b_l, c_j и потому переходящие в себя при применении φ_{ijk}. Выписанные же два соотношения при применении φ_{ijk} переходят в следствия соотношений в K_0: первое в

$$t_k^{-1}\, a_i\, b_l\, c_i\, t_k = a_i\, b_l\, c_i,$$

а второе — в

$$t_k^{-1}\, t_k\, c_j\, t_k = t_k\, c_j.$$

Остается учесть, что $l \neq k$ и $j \neq k$.

Из определения K видно, что K конечно определена; из свойств HNN-расширений — что $\overline{G} \subseteq K$.

5.7. Конструкция подгрупп $L_s \subseteq K$.

Вид подгруппы L_s будет зависеть от уравнения, определяющего множество E_s (п. 5.4)

Определим запас групп, среди которых содержатся все L_s:

$$L_i^c = \left|\left\{a(0 \ldots \underbrace{0}_{i}\, c\, 0 \ldots 0),\ t_r\ (r \neq i)\right\}\right|,$$

$$L_{ij}^{=} = |\{a(0 \ldots 0),\ t_l\, t_j,\ t_r\ (r \neq i,\ j)\}|,$$

$$L_{ijk}^{+} = |\{a(0 \ldots 0),\ t_i t_k,\ t_j\, t_k,\ t_r\ (r \neq i,\ j,\ k)\}|,$$

$$L_{ijk}^{\times} = |\{a(0 \ldots 0),\ t_{ijk},\ t_{jik},\ t_r\ (r \neq i,\ j,\ k)\}|,$$

и аналогично в обозначениях 5.5

$$\overline{H}_i^c = |\{a(x_0, \ldots, x_m),\ x_i = c\}|,$$

$$\overline{H}_{ij}^{=} = |\{a(x_0, \ldots, x_m),\ x_i = x_j\}|,$$

$$\overline{H}_{ijk}^{+} = |\{a(x_0, \ldots, x_m),\ x_k = x_j + x_i\}|,$$

$$\overline{H}_{ijk}^{\times} = |\{a(x_0, \ldots, x_m),\ x_k = x_j \cdot x_i\}|.$$

Ясно, что L_s конечно порождены. Остается последняя серия проверок:

5.8. $\overline{H}_i^c = \overline{G} \cap L_i^c$, $\overline{H}_{ij}^{=} = \overline{G} \cap L_{ij}^{=}$ и т. д.

Прежде всего из (1) — (3) находим

$$t_i^{-1}\, a(x_0, \ldots, x_m)\, t_i = a(x_0, \ldots, x_{i-1}, x_i + 1, x_{i+1}, \ldots, x_m); \tag{4}$$

$$t_{ijk}^{-1}\, a(x_0, \ldots, x_m)\, t_{ijk} = a(y_0, \ldots, y_m), \tag{5}$$

где $y_i = x_i + 1$, $y_k = x_k + x_j$, $y_s = x_s$ при $s \neq i, k$

(при проверке последнего равенства учесть, что $k \geqslant l + 1$, так что t_k коммутирует со средней частью слова $a(x_0, \ldots, x_m)$, состоящей из $\bar{a}_i$, $\bar{b}_i$, $\bar{c}_i$, $i \leqslant l$).

Отсюда следует, что

$$L_1^c = |\bar{H}_i^c \cup \{t_r \mid r \neq i\}|,$$

$$L_{ij}^{=} = |\bar{H}_{ij}^{=} \cup \{t_i t_j, t_r \mid r \neq i, j\}|,$$

$$L_{ijk}^{+} = |\bar{H}_{ijk}^{+} \cup \{t_i t_k, t_j t_k, t_r \mid r \neq i, j, k\}|,$$

$$L_{ijk}^{\times} = |\bar{H}_{ijk}^{\times} \cup \{t_{ijk}, t_{jik}, t_r \mid r \neq i, j, k\}|.$$

В самом деле, включения $\subseteq$ очевидны. Далее, начав с $a(x_0, \ldots, x_m)$ и применив сопряжение посредством t_r, мы можем как угодно изменить r-ю координату в силу (4): это сразу дает включение $L_i^c \supseteq H_i^c$ и потому требуемое равенство. Аналогично проверяется второе равенство.

Третье: сопряжение с помощью $t_i t_k$ увеличивает i-ю и k-ю координаты на 1, а с помощью $t_j t_k$ — j-ю и k-ю, потому что можно получить любой вектор с $x_k = x_j + x_i$ исходя из нулевых координат на этих местах.

Четвертое: сопряжение с помощью t_{ijk} увеличивает x_i на 1, x_k на x_j; t_{jik} аналогично, что позволяет получить любой вектор с $x_k = x_j x_k$ исходя из нулевого.

Эта новая характеризация групп L_s показывает, что $L_s \cap \bar{G} \supseteq H_s$ для всех s. Остается установить обратное включение.

С этой целью заметим, что любой элемент из L_s с помощью соотношений (4) и (5) может быть представлен в виде Th, где $T \in |\{t_i, t_{ijk}\}|$ (набор допустимых индексов i, ijk зависит от s) и $h \in H_s$ (то же рассуждение, что и выше). Но по предложению 2.7 а) все $\{t_i, t_{ijk}\}$ порождают свободную подгруппу, имеющую тривиальное пересечение с $\bar{G}$ (см. доказательство 2.7а)). Следовательно, если $Th \subseteq \bar{G}$, то $T = 1$ и $h \in H_s$, что завершает доказательство.

6. ОКОНЧАНИЕ ДОКАЗАТЕЛЬСТВА

6.1. В этом параграфе заканчивается проверка посылки предложения 4.3 и тем завершается доказательство теоремы Хигмэна.

Положим $G = |\{a, b\}|$ и пусть $H \subseteq G$ — перечислимая подгруппа. Мы покажем, что H хороша. Первый шаг состоит в редукции задачи к доказательству того, что хороша некоторая конкретная подгруппа

$$H' \subset G' \cong \overset{?}{*}_1 Z,$$

не зависящая от H. Чтобы определить H', введем сначала рекурсивное (бесконечное) перечисление $\gamma : Z^+ \to \bar{G}$

$$\gamma(2^{m_0} 3^{m_1} \ldots p_r^{m_r}) = \prod_{i=0}^{\infty} a^{m_{4i} - m_{4i+1}} b^{m_{4i+2} - m_{4i+3}}.$$

После этого положим

$$G' = |\{a, b, t, v, c, d, e\}|,$$

$$\tau: S(\{a, b, a^{-1}, b^{-1}\}) \to G': \prod_{i \geqslant 0} a^{m_{2i}} b^{m_{2i+1}} \to t \prod_{i \geqslant 0} (v^{-i} a v^i)^{m_{2i}} (v^{-i} b v^i)^{m_{2i+1}},$$

$$H' = |\{\tau(g) c^n d e^n \mid g \in S(\{a, b, a^{-1}, b^{-1}\}),\ n \in Z+,\ g = \gamma(n)\}| \subseteq G'.$$

Выписанная формула определяет τ на не обязательно приведенных словах, и приведение может изменить τ-образ.

Слово $\tau(g) c^n d e^n$, образующее H', однозначно определяется по своему номеру n.

6.2. Лемма. *Если $H' \subset G'$ хорошая подгруппа, то любая перечислимая подгруппа $H \subseteq G$ хорошая.*

Доказательство. а) Положим

$$H' = |\{\tau(h) c^n d e^n \mid \text{образ } h \in H,\ n \in Z+,\ h = \gamma(n)\}| \subseteq H'.$$

Тогда

$$H'' = H' \cap |\{a, b, t, v, c^n d e^n \mid n \in \gamma^{-1}(H)\}|.$$

В самом деле, включение $\subseteq$ очевидно. Обратное включение следует из того, что множество образов элементов $c^n d e^n$, $n \geqslant 1$, в факторе G' по ядру, порожденному a, b, t, v, свободно. Поэтому по каждому приведенному слову от образующих $\tau(g)\, c^n d e^n$ последовательность номеров n этих образующих восстанавливается однозначно; и если все они лежат в $\gamma^{-1}(H)$, то слово лежит в H''.

Значит, H'' есть пересечение H' с подгруппой, порожденной ограниченным перечислимым множеством образующих ($\gamma^{-1}(H)$ перечислимо вместе с H). Поэтому
H'' хороша, если H' хороша.

б) Положим

$$\bar{H} = |\{\tau(h) \mid h \in H\}| \subseteq G'.$$

Легко убедиться, что

$$|\bar{H} \cup \{c, d, e\}| = |H'' \cup \{c, d, e\}|.$$

Поэтому

$$\bar{H} = |H'' \cup \{c, d, e\}| \cap |\{a^{-i} b, v, t\}|.$$

По лемме 4.4 $\bar{H}$ хороша, если H'' хороша.

в) Наконец, рассмотрим гомоморфизм $\varphi: G' \to G$ переводящий a, b в себя, t, v, c, d, e в 1. Очевидно, $\varphi(\bar{H}) = H$. По лемме 4.5 H хороша, если $\bar{H}$ хороша.

6.3. Приступим к доказательству того, что подгруппа $H' \subset G'$ хорошая. С этой целью построим коммутативную диаграмму вложений групп

$$\begin{array}{ccccc} G' & \to & K & \to & K \\ \uparrow & & \uparrow & & \uparrow \\ H' & \to & L' & \to & L \end{array}$$

со следующими свойствами:

а) K определена конечным множеством образующих и ограниченным перечислимым множеством соотношений; L порождена ограниченным перечислимым множеством слов в образующих K;

б) $L' \to L$ есть изоморфизм;

в) $H' = G' \cap L'$ в K'.

Отсюда следует, что H' хороша. В самом деле, пусть $K = F/\overline{R}$, где F — свободная группа, порожденная конечной системой образующих K; R_0 — ограниченное перечислимое множество соотношений между ними, а $\overline{R}$ — порожденный ими нормальный делитель. Из предложения 5.2 следует, что R_0 порождает хорошую подгруппу R в F, а из леммы 4.2 тогда вытекает, что $K = F/\overline{R}$ вкладывается в к.о. группу M. При этом вложении ограниченное перечислимое множество образующих L остается таким в M (относительно образующих M) и потому $L \subset M$ хороша по следствию предложения 5.2. Отсюда в силу б), в) имеем: подгруппа $H' = G' \cap L$ хороша вместе с G и L как подгруппа M. Значит, есть вложение (M, H') в $(\overline{M}, \overline{H})$, такое, что $\overline{M}$ конечно определена, $\overline{H}$ конечно порождена и $H' = \overline{H} \cap M$. Это вложение индуцирует вложение пары (G', H') в $(\overline{M}, \overline{H})$ с теми же свойствами. Следовательно, H' хороша и в G'.

Остается построить указанную диаграмму и доказать свойства а) — в).

6.4. Группа K'. Это — кратное HNN-расширение группы G', определенное, как в предложении 2.7, с помощью четырех счетных последовательностей нетривиальных изоморфизмов подгруппы $\langle\{t, c, d, e, v^{-t}av^t, v^{-t}bv^t \mid i \geqslant 0\} \mid \subset G'$ в G'. Так как выписанные элементы свободно порождают эту подгруппу, достаточно указать, во что они переводятся интересующими нас изоморфизмами. В K' эти изоморфизмы будут индуцированы сопряжением посредством четырех последовательностей образующих x_i, $\bar{x}_i$, y_i, $\bar{y}_i$, $i \geqslant 0$ (вместо t_i, $i \in I$ в обозначениях § 2). В следующей таблице указано их действие. Обозначения: $a_i = v^{-t}av^t$, $b_i = v^{-t}bv^t$, p_j — j-е простое число. Элемент таблицы, стоящий на пересечении, скажем, строки c и столбца $\bar{x}_t$, есть $\bar{x}_t^{-1} c\, x_t$.

	x_t	$\bar{x}_t$	y_t	$\bar{y}_t$
t	ta_i	ta_i^{-1}	b_i	tb_i^{-}
c	$c^{p_{4i}}$	$c^{p_{4i+1}}$	$c^{p_{4i+2}}$	$c^{p_{4i+3}}$
d	d	d	d	d
e	$e^{p_{4i}}$	$e^{p_{4i+1}}$	$e^{p_{4i+2}}$	$e^{p_{4i+3}}$
a_j	$\begin{cases} a_i^{-1} a_j a_i, & j < i \\ a_j, & j \geqslant i \end{cases}$	$\begin{cases} a_i a_j a_i^{-1}, & j < i \\ a_j, & j \geqslant i \end{cases}$	$\begin{cases} b_i^{-1} a_j b_i, & j < i \\ a_j, & j \geqslant i \end{cases}$	$\begin{cases} b_i a_j b_i^{-1}, & j < i \\ a_j, & j \geqslant i \end{cases}$
b_j	$\begin{cases} a_i^{-1} b_j a_i, & j < i \\ b_j, & j \geqslant i \end{cases}$	$\begin{cases} a_i b_j a_i^{-1}, & j < i \\ b_j, & j \geqslant i \end{cases}$	$\begin{cases} b_i^{-1} b_j b_i, & j < i \\ b_j, & j \geqslant i \end{cases}$	$\begin{cases} b_i b_j b_i^{-1}, & j < i \\ b_j, & j \geqslant i \end{cases}$

Окончательно положим

$K' = \langle G' \cup \{x_i, \bar{x}_i, y_i, \bar{y}_i \mid i \geqslant 0\}$: соотношения из таблицы $\rangle$, $G' \to K'$ — естественное вложение.

6.5. Группа L'. Положим

$$L' = |\{tcde, x_i, \bar{x}_i, y_i, \bar{y}_i \mid i > 0\}| \subseteq K',$$

$L' \to K'$ — естественное вложение. Проверка того, что H' вкладывается в L' (по коммутативности диаграммы, как подгруппа K'), будет проведена в п.6.7.

6.6. Группы K, L. Положим

$$K = |G' \cup \{u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4\} : R|,$$

где соотношения R и вложение $K' \to K$ одновременно определяются следующими условиями:

R=образ табличных соотношений после подстановки в них

$$x_i \to u_1^{-i} v_1 u_1^i, \quad \bar{x}_i \to u_2^{-i} v_2 u_2^i$$

$$y_i \to u_3^{-i} v_3 u_3^i, \quad \bar{y}_i \to u_4^{-i} v_4 u_4^i,$$

$K' \to K$ — гомоморфизм, тождественный на G' и действующий на остальные образующие этими подстановками. Гомоморфизм $K' \to K$ является вложением. Действительно, элементы $u_j^{-i} v_j u_j^i$ в $|\{u_j, v_j\}|$ свободны, поэтому K можно рассматривать как свободное произведение K' и $|\{u_j, v_j \mid 1 \leqslant j \leqslant 4\}|$ с объединенными согласно выписанным подстановкам подгруппами (учесть предложение 2.7а)).

Наконец, положим

L-образ L' при вложении $K' \to K$.

6.7. Диаграмма построена. Утверждение 6.4а), б) для нее проверяется непосредственно из определений. Остается доказать, что $H' = G' \cap L'$ в K'.

а) Положим $[n] = \tau(g)\, c^n d e^n$ для $n \in Z+$, $g = \gamma(n)$ в обозначениях п. 6.1. Напомним, что H' порождена всеми $[n]$ в G' и, значит, в K'.

Таблица соотношений в K' была придумана так, чтобы выполнялись следующие тождества:

$$x_i^{-1}\,[n]\,x_i = [p_{4i}\, n], \quad \bar{x}_i^{-1}\,[n]\,\bar{x}_i = [p_{4i+1}\, n],$$

$$y_i^{-1}\,[n]\,y_i = [p_{4i+2}\, n], \quad \bar{y}_i^{-1}\,[n]\,\bar{y}_i = [p_{4i+3}\, n].$$

В самом деле, проверим, скажем, первое из них. Пусть тогда согласно определениям

$$\gamma(n) = \prod_j a^{m_{4j} - m_{4j+1}} b^{m_{4j+2} - m_{4j+3}},$$

$$[n] = t \prod_j a_j^{m_{4j} - m_{4j+1}} b_j^{m_{4j+2} - m_{4j+3}} c^n d e^n,$$

откуда по первому столбцу таблицы в п. 6.4:

$$x_i^{-1}\,[n]\,x_i = t a_i \cdot a_i^{-1} \prod_{j<i} (\ldots)_j\, a_i \prod_{j \geqslant i} (\ldots)_j\, c^{p_{4i}\, n} d e^{p_{4i}\, n} = [p_{4i}\, n].$$

Учитывая еще, что $[1] = tcde \in L'$, из этих формул сопряжения получаем, что $[n] \in L'$ для всех n и $H' \subset L'$, как было обещано в п. 6.5. Сверх того

$$|H' \cup \{x_i, \bar{x}_i, y_i, \bar{y}_i \mid i > 0\}| = L'$$

включение $\subseteq$ проверено, а обратное очевидно.

б) Покажем теперь, что в K'

$$|H' \cup \{x_i, \bar{x}_i, y_i, \bar{y}_i \mid i \geqslant 0\} \mid \cap G' = H^*.$$

Так как K' является HNN-расширением G', достаточно установить, что мы находимся в ситуации, когда выполнены условия предложения 2.7 (они описаны в конце п. 2.6) и применить утверждение 2.7б).

Проверим эти условия, скажем, для первой серии изоморфизмов подгруппы G', описанной в начале п. 6.4. Эта серия отвечает сопряжению посредством x_i в K'. В нашем случае условия принимают следующий вид:

$$x_i^{-1} |H' \cap | \{t, c, d, e; a_j, b_j \mid j \geqslant 0\} | | x_i = H' \cap x_i^{-1} | \{t, c, d, e; a_j, b_j \mid j \geqslant 0\} | x_i,$$

т. е. по определению H' и таблице

$$x_i^{-1} H' x_i = H' \cap \left| \left\{t, c^{p_{4i}}, d, e^{p_{4i}}; a_j, b_j \,\middle|\, j \geqslant 0\right\} \right|.$$

Так как $x_i^{-1} [n] x_i = [p_{4i} n]$, включение $\subseteq$ очевидно. Наоборот, пусть задан элемент из H', записанный как приведенное слово в образующих $[n]$: $\prod_{j \geqslant 0} [n_j]^{\mathscr{E}_j}$, $\mathscr{E}_j = \pm 1$. Рассмотрим соответствующее ему приведенное слово g в G'.

Покажем, что если c, d входят в g только в степенях, делящихся на p_{4i}, то среди $[n_j]$, $\mathscr{E}_j \neq 0$, все n_j делятся на p_{4i}, т. е. $[n_j] \in x_i^{-1} H' x_i$.

В самом деле, пусть $\bar{g}$ = образ g в $| \{c, d, e\} |$ при гомоморфизме, переводящем t, a_j, b_j в 1. Так как $[\bar{n}] = c^n d e^n$, то все $[\bar{n}]$ свободны, и последовательность $\{\mathscr{E}_j n_j\}$ однозначно восстанавливается по $\bar{g}$. Нетрудно убедиться, что формулы, выражающие $\mathscr{E}_j n_j$ через степени, с которыми c, e входят в приведенное слово $\bar{g}$, линейны с целыми коэффициентами (точнее, это дизъюнкции линейных формул, сопровожденных условиями типа неравенств). Поэтому из делимости всех этих степеней на p_{4i} следует и делимость n_j на p_{4i}.

Это завершает доказательство.

ЗАКЛЮЧЕНИЕ

В сентябре 1979 года в Ургенче, центре Хорезмской области Узбекистана, состоялся международный симпозиум математиков «Алгоритм в современной математике и ее приложениях». Местом его проведения была выбрана родина великого ученого IX века Мухаммеда аль-Хорезми (то есть «хорезмийца»). Мы уже упоминали во Введении, что к имени аль-Хорезми восходит термин «алгоритм» (а к названию составленного им учебника — слово «алгебра»). Трактат аль-Хорезми был написан по-арабски; среди прочего в нем была описана индийская позиционная система записи числе и приемы вычислений в такой записи. Латинская версия трактата, относящаяся к XII веку, начинается словами «Dixit algorizmi», то есть «Сказал аль-Хорезми».

Воздух Хорезмского оазиса и древнее радушие хозяев не только способствовали успеху симпозиума в том техническом смысле этого слова, как его понимают обычно, но заставили участников воспринимать математику одновременно более исторически и более личностно. Абстрактная математическая процедура, гарантией ценности которой для современника служит именно ее защищенность от произвола индивидуального сознания, вдруг предстала в Ургенче почти как поэтический феномен, зачатый и поддержанный авторитетом творческой мысли конкретного человека.

XII век не был случайным временем в истории европейской культуры. Французский медиевист Марк Блок в своей книге «Я феодальное общество» (см. М. Блок, «Апология истории», М. Наука 1973) широкими мазками набрасывает картину общества, которое именно в это время все активнее начинает последовательно рассуждать о себе самом.

«Можно ли считать несущественным в еще полной загадок истории связей между мыслью и практикой тот факт, что к концу второго феодального периода люди действия обычно располагали более совершенным, чем прежде, инструментом логического анализа?» (М. Блок, loc. cit., стр. 159). В этой фразе историк общественных отношений вовсе не имеет в виду именно трактат аль-Хорезми, но, вглядываясь в развернутую им панораму, мы начинаем лучше различать время, когда правила сложения столбиком могли впервые стать социальным явлением.

Участие в симпозиуме «Алгоритм» побудило автора этой книжки еще раз задуматься о том, что ее заглавие могло бы обещать

много больше, чем предложенное читателю жесткое изложение нескольких (в самом деле замечательных) теорем и понятий теории рекурсивных функций. Например, следовало бы тщательно проанализировать представление о конструктивном (или вычислительном) универсуме, которое является одной из полуоформившихся абстракций теории вычислимости. Такой универсум — это потенциально счетное множество объектов, которые можно эффективно строить и эффективно различать с помощью операций из фиксированного конечного списка. Алгоритмы в универсуме осуществляют переработку одних конструктивных объектов в другие. Нумерации Геделя и отождествление алгоритмов (результатов их работы) с частично рекурсивными функциями можно интерпретировать как универсальный способ устанавливать изоморфизм между любыми двумя конструктивными универсумами. Но изоморфизм не есть тождество, и одна из главных возможностей теории универсумов состоит в систематическом рассмотрении расширений. На языке теории рекурсивных функций идея такого расширяющегося конструктивного универсума приводит к вопросам, которые в книге даже не поставлены. Арифметический универсум Z_+, основной прототип и модель всех универсумов, предстает в роли, важность которой, может быть, преувеличена.

В гносеологическом плане многое можно было бы сказать о соотношении понятий «вычислимость» и «познаваемость». Первое из них относится только к проработке избранной математической модели действительности, будь то система дифференциальных уравнений или задача выпуклого программирования. Второе же много шире, поскольку и сам выбор модели, и задача проверки ее адэкватности находятся далеко за пределами алгоритмического мира. Поставленный на симпозиуме вопрос «Что делать после того, как неразрешимость массовой задачи доказана?» был и приглашением взглянуть на этот мир извне.

Но все это — «мысли на лестнице». Автор откладывает шариковую ручку в надежде, — общей для всех пишущих, — что кто-нибудь додумает их за него.

СПИСОК ЛИТЕРАТУРЫ

1. **Успенский В. А.** Лекции о вычислимых функциях. М.: Физматгиз, 1960.
2. **Роджерс Х.** Теория рекурсивных функций и эффективная вычислимость Пер. с англ./Под ред. В. А Успенского.— М.: Мир, 1972.
3. **Мальцев А. И.** Алгоритмы и рекурсивные функции.— М.: Наука, 1966.
4. **Марков А. А.** Теория алгоритмов.— Труды/Математический ин-т им. В. А. Стеклова АН СССР, 1954, т. 42.
5. **Ершов Ю. Л.** Теория нумераций.— М.: Наука, 1977.
6. **Сложность** вычислений и алгоритмов: Пер. с англ./Под ред. В. А. Козмидиади, А. Н. Маслова, В. Н. Петри.— М.: Мир, 1974.
7. **Машины Тьюринга** и вычислимые функции: Пер. с нем.— М.: Мир, 1972.
8. **Криницкий Н. А.** Алгоритмы вокруг нас.— М.: Наука, 1977.
9. **Успенский В. А.** Машины Поста.— М.: Наука, 1979.
10. **Тростников В. А.** Конструктивные процессы в математике.— М.: Наука, 1975.
11. **Ершов А. П.** Введение в теоретическое программирование.— М.: Наука, 1977.
12. **Дейкстра Э.** Дисциплина программирования: Пер. с англ./ Под ред. Э. З. Любимского.— М.: Мир, 1978.
13. **Манин Ю. И.** Доказуемое и недоказуемое.— М.: Сов. радио, 1979.
14. **Мельчук И. А.** Опыт лингвистических моделей «Смысл ↔ Текст». — М.: Наука, 1974.
15. **Апресян Ю. Д., Богуславский И. М., Иомдин Л. Л., Крысин Л. П., Лазурский А. В., Перцов Н. В., Санников В. З.** Лингвинистическое обеспечение в системе автоматического перевода третьего поколения.— М.: АН СССР На учный совет по комплексной проблеме «Кибернетика», 1978.
16. **Роллер Э.** Открытие основных законов жизни: Пер. с англ./ Под ред. В. М. Родионова.— М.: Мир, 1978.
17. **Поплавский Р. П.** Термодинамические модели информационных процессов. — УФН. 1975, т. 115, вып. 3, с. 465—501.
18. **Матиясевич Ю. В.** Диофантовы множества.— УМН, 1972. т. 22, вып. 5, с. 185—222.
19. **Колмогоров А. Н.** Три подхода к определению понятия «количество информации».— Проблемы передачи информации, 1965, т. 1, вып. 1, с. 3—7
20. **Колмогоров А. Н.** К логическим основам теории информации и теории вероятностей.— Проблемы передачи информации, 1969, т. 5, вып. 3, с. 3—7.
21. **Звоикин А. К., Левин Л. А.** Сложность конечных объектов и обоснование понятий информации и случайности с помощью теории алгоритмов.— УМН 1970, т. 25, вып. 6, с. 85—127
22. **Jones J. P., Sato D., Wada H., Wiens D.** Diophantine representation of the set of prime numbers.— Amer. Mathem. Monthly, 1976, v. 83, № 6, p. 449—464.
23. **Davis M., Matijasevic Ju. Robinson J.** Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution. — Proc. of Symposia in Pure Mathem., v. XXIII, 1976, Providence, Rhode Island, p. 323—378.
24. **Paris J., Harrington L.** A mathematical incompleteness in Peano arithmetic.— — Handbook of Mathem. Logic, North Holland, Amsterdam, 1978.

25. **Петер Р.** Рекурсивные функции: Пер. с англ./Под ред. В. А. Успенского.— М.: ИЛ, 1954.
26. **Клини С.** Введение в математику: Пер. с англ./Под ред. В. А. Успенского.— — М.: ИЛ, 1957.
27. **Feferman S.** Transfinite recursiwe progressions of axiomatic theories.— J. Symb. Logic, 1972, v. 27, № 3, p. 259—316.
28. **Higman G.** Sybgroups of finitely presented groups.— Proc. Royal Soc., Ser. A., 1961, v. 262, p. 455 — 475.
29. **Валиев М. К.** Примеры универсальных конечно определенных групп. — ДАН СССР, 1973, т. 211, № 2, с. 265—268.
30. **Серр Ж.-П.** Деревья, амальгамы и SL_2.— Математика, 1974, т. 18, вып. 1, с. 3—51.
31. **Постников М. М.** Теорема Ферма.— М., Наука, 1978.
32. **Ахо А., Хопкрофт Дж., Ульман Дж.**— Построение и анализ вычислительных алгоритмов: Пер. с англ./ Под ред Ю. В. Матиясевича. — М.: Мир, 1979.

ИМЕННОЙ УКАЗАТЕЛЬ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ

Юрий Иванович Манин

ВЫЧИСЛИМОЕ И НЕВЫЧИСЛИМОЕ

Редактор Н. Д. Иванушко
Художественный редактор Н. А. Игнатьев
Технический редактор Т. Н. Зыкина
Корректор Н. Н. Васина

ИБ № 623

Сдано в набор 26.05.80. Подписано в печать 9.10.80 Т-14876
Формат 60×84¹/₁₆. Бумага книжно-журн. № 3. Гарнитура литературная.
Печать высокая. Объем 7,44 усл. п. л. 7,99 уч.-изд. л. Тираж 25 000 экз.
Заказ 1873. Цена 45 к.
Издательство «Советское радио», Москва, Главпочтамт, а/я 693
Московская типография № 4 Союзполиграфпрома Государственного комитета СССР по делам издательств, полиграфии и книжной торговли.
129041, Москва, Б. Переяславская ул., д. 46.