«СОВРЕМЕННАЯ МАТЕМАТИКА»

Популярная серия

Машины Тьюринга и рекурсивные функции

Г.-Д. Эббинхауз, К. Якобс
Ф.-К. Ман, Г. Хермес

Перевод с немецкого

Э. Г. Белаги

ИЗДАТЕЛЬСТВО «МИР»
Москва 1972

Selecta Mathematica II

Herausgegeben von KONRAD JACOBS

H.-D. Ebbinghaus
Turing-Maschinen und berechenbare Funktionen I

F.-K. Mahn
Turing-Maschinen und berechenbare Funktionen II

H.-D. Ebbinghaus
Turing-Maschinen und berechenbare Funktionen III

H.-D. Ebbinghaus
Aufzählbarkeit

H. Hermes
Entscheidungsproblem und Dominospiele

K. Jacobs
Turing-Maschinen und zufällige 0-1-Folgen

K. Jacobs
Maschinenerzeugte 0-1-Folgen

SPRINGER-VERLAG
Berlin · Heidelberg · New York
1970

«СОВРЕМЕННАЯ МАТЕМАТИКА»

Популярная серия

Машины Тьюринга и рекурсивные функции

Г.-Д. Эббинхауз, К. Якобс
Ф.-К. Ман, Г. Хермес

Перевод с немецкого

Э. Г. Белаги

ИЗДАТЕЛЬСТВО «МИР»

Москва 1972

УДК 517.11

Этот коллективный труд немецких математиков содержит элементарное изложение теории машин Тьюринга и рекурсивных функций — важного раздела современной математической логики, нашедшего широкое применение в кибернетике. Помимо основ этой теории, книга содержит ряд существенных результатов, включая достижения последнего времени (в частности, результаты Колмогорова о связи машин Тьюринга с основаниями теории вероятностей). Изложение ведется строго, но доступно, содержит много примеров и пояснений.

Книгу с интересом прочтут читатели разных категорий, начиная от учащихся старших классов школ с математической специализацией и кончая научными работниками и преподавателями высшей школы.

Редакция литературы по математическим наукам

$\frac{2\text{-}2\text{-}3}{37\text{-}72}$

МАШИНЫ ТЬЮРИНГА И РЕКУРСИВНЫЕ ФУНКЦИИ

Г.-Д. Эббинхауз, К. Якобс, Ф.-К. Ман, Г. Хермес

Редактор *Н. И. Плужникова* Художник *А. В. Шипов*
Художественный редактор *В. И. Шаповалов*
Технический редактор *Е. Д. Кузнецова* Корректор *К. Л. Водяницкая*
Сдано в набор 17/IV 1972 г. Подписано к печати 6/IX 1972 г.
Бумага №1 $84\times108^1/_{32}$=4,13 бум. л. 13,86 усл. печ. л.
Уч.-изд. л. 12,41. Изд. № 1/6656. Цена 89 к. Зак. 2901

ИЗДАТЕЛЬСТВО «МИР»
Москва, 1-й Рижский пер., 2

Ордена Трудового Красного Знамени Первая Образцовая типография имени А. А. Жданова Главполиграфпрома Государственного комитета Совета Министров СССР по делам издательств, полиграфии и книжной торговли
Москва, М-54, Валовая, 28.

ОТ ПЕРЕВОДЧИКА

Предлагаемая вниманию читателей книга Г.-Д. Эббингауза, К. Якобса, Ф.-К. Мана и Г. Хермеса «Машины Тьюринга и рекурсивные функции» представляет собой перевод второго томика серии «Selecta Mathematica»; в русское издание включена также статья К. Якобса «Машинно-порожденные 0-1-последовательности» из первого томика той же серии.

Серия «Selecta Mathematica» задумана ее редактором и одним из авторов Конрадом Якобсом, профессором Математического института университета Эрлангена — Нюрнберга, как собрание математических текстов, доступных студентам начальных курсов и преподавателям математики средних школ и позволяющих на вполне строгом уровне познакомиться с отдельными интересными современными результатами.

Обзор содержания книги дан в предисловии. В отечественной популярной и, пожалуй, специальной литературе до сих пор не было столь подробного и прозрачного изложения теории вычислимости по Тьюрингу и смежных вопросов рекурсивной теории и математической логики; жемчужиной книги, безусловно, является доказательство теоремы А. Тарского о неразрешимости арифметики, хотя именно эта теорема потребует от читателя наибольших усилий.

Некоторые результаты, изложенные в книге, публиковались до сих пор лишь в специальных научных журналах и впервые становятся достоянием широкой аудитории читателей, интересующихся математикой; по-видимому, они будут интересны и специалистам. К их числу относятся: теоремы Хао Вана, А.-С. Кара и др. о неразрешимости некоторых проблем игры «квадратное домино»; исследования А. Н. Колмогорова и П. Мартин-Лёфа о случайных 0-1-последовательностях; результаты М. Морса, Г. Хедлунда и др. авторов (1922—1967 гг.) о построении и периодических (точнее, квазиэргодических) свойствах конечных и бесконечных 0-1-последовательностей (их изложение завершается списком задач, частью еще не решенных).

Выбор перечисленных в предыдущем абзаце тем и их трактовка в таком доступном и одновременно вполне строгом стиле представляются очень удачными: начиная от математических безделушек вроде «вальса бесконечного порядка» (тернарная последовательность М. Кини) и кончая универсальным секвенциальным тестом П. Мартин-Лёфа («сито», сквозь которое просеиваются случайные бесконечные последовательности нулей и единиц) — все эти впервые популяризируемые результаты интересны и элегантны.

Тем читателям, которые захотят углубить свое знакомство с разделами, в той или иной степени освещенными в этой книжке, можно порекомендовать следующий список литературы:

по теории рекурсивно-вычислимых функций:

Петер Р., Рекурсивные функции, ИЛ, М., 1954.

Успенский В. А., Лекции о вычислимых функциях, Физматгиз, М., 1960;

по математической логике:

Новиков П. С., Элементы математической логики, Физматгиз, М., 1959;

Линдон Р., Заметки по логике, изд. «Мир», М., 1968;

по теории алгоритмов и вычислительных устройств:

Марков А. А. Теория алгоритмов, Изд. АН СССР, М., 1954.

Трахтенброт А. Б., Алгоритмы и машинное решение задач, М., 1960;

по теории формальных языков:

статьи Н. Хомского (см. Кибернетический сб., вып. 1, 2, 3, 6, изд. «Мир»);

по основаниям теории вероятностей:

Колмогоров А. Н., Основные понятия теории вероятностей, М.—Л., 1936;

Мизес С., Вероятность и статистика, М.—Л., 1930.

по эргодической теории:

Биллингслей, Эргодическая теория и информация, изд. «Мир»., М., 1969.

Все другие литературные источники, добавленные переводчиком, помещены в конце списка литературы к соответствующим статьям и отмечены звездочкой.

Э. Белага

ПРЕДИСЛОВИЕ

Хочется надеяться, что эта книга найдет читателей, готовых на некоторые усилия для того, чтобы войти в круг идей теории рекурсивных функций — теории, одним из замечательных результатов которой является, например, теорема Гёделя о неполноте. Речь идет о вопросах, при обсуждении которых наш обыденный язык становится неоднозначным и недостаточно точным; он обладает привлекательной, но для наших целей губительной способностью выражать разнообразные смысловые оттенки и сложные намеки. Это наводит на мысль построить некий сакральный (или, говоря более прозаично, формальный) язык, обладающий небольшим, но достаточным для нашего исследования запасом символов (логических, например) и немногими правилами их соединения, так чтобы его использование гарантировало точность и однозначность выводов. Помимо этого, мы опишем устройство и действие так называемых машин Тьюринга, каждая из которых работает согласно своему неизменному закону вдоль неограниченной в одну сторону писчей ленты: печатает на ней, стирает прежние записи и, возможно, прекращает работу после получения решения.

В статье «Машины Тьюринга и вычислимые функции I—III» Г.-Д. Эббинхауза и Ф.-К. Мана теория этих машин развивается, начиная с основ; среди прочих результатов доказывается теорема Клини о перечислимости и конструируется универсальная машина Тьюринга. Среди применений — несколько важных результатов о неразрешимости.

Статья «Перечислимость» Г.-Д. Эббинхауза посвящена машинно-порождаемым множествам. Излагается более общий вариант теоремы Клини о перечислимости, а также доказательство того факта, что истинные предложения арифметики не могут быть машинно-порождены.

Уточнение идеи разрешимости стало источником большого числа исследований. Так, Ван поставил вопрос о том, имеет ли решение известная игра «домино». Здесь возникает поразительная связь с классической проблемой разрешимости логики предикатов. Об этом рассказывается в статье Г. Хермеса «Проблема разрешимости и игра «домино»».

Подробному изложению основных идей новейших исследований А. Н. Колмогорова и П. Мартин-Лёфа о перечислимости и случайности посвящена моя статья «Машины Тьюринга и случайные 0-1-последовательности».

Машины Тьюринга реализуют лишь одну из многих возможностей точного выражения понятий перечислимости и вычислимости. В статье Г.-Д. Эббинхауза показывается, что использование так называемых систем правил, или исчислений, приводит к тому же результату. У машин Тьюринга есть, однако, методическое преимущество большой наглядности, и поэтому в нашем изложении они стоят на переднем плане. Остается лишь пожалеть о том, что их нет в продаже. Можно, однако, промоделировать машины Тьюринга на обычных счетных устройствах, и это уже сделано. Мы видим, как тесно соприкасаются чисто теоретические исследования с технической задачей обработки данных. Сами машины Тьюринга могут рассматриваться как идеализированные счетные устройства.

В соответствии с принципом «Selecta Mathematica» и в этом томике все существенные результаты сопровождаются полными доказательствами. Тем самым мы надеемся дать читателям основательное представление о мире абстрактных автоматов и побудить их познакомиться и с практическими аспектами теории.

Колумбус, январь 1970 г.

Конрад Якобс,
редактор

МАШИНЫ ТЬЮРИНГА И ВЫЧИСЛИМЫЕ ФУНКЦИИ I
УТОЧНЕНИЕ ПОНЯТИЯ АЛГОРИТМА

Г.-Д. ЭББИНХАУЗ

Настоящая статья является введением в круг вопросов, связанных с уточнением понятия вычислимости. Исходя из интуитивных представлений, мы проводим анализ понятия алгоритма и мотивируем введение понятия функции, вычислимой по Тьюрингу. В следующей статье Ф.-К. Мана «Машины Тьюринга и вычислимые функции II» рассматриваются конкретные примеры функций, вычислимых по Тьюрингу, и обосновывается целый ряд методов, существенных для работы с машинами Тьюринга (диаграммы, нормированное вычисление). В заключение доказываются некоторые теоремы о неразрешимости. В третьей статье «Машины Тьюринга и вычислимые функции III» будет описана конкретная, в определенном смысле универсальная машина Тьюринга и будет доказана теорема Клини о перечислимости для функций, вычислимых по Тьюрингу.

В первых трех статьях дана сплошная нумерация параграфов. Литературные ссылки относятся к библиографии, приведенной в конце третьей статьи.

§ 1. *Нестрогие предварительные соображения*

1. Алгоритмы в математике. Исторические замечания

Под *алгоритмом* [1]) для некоторого класса задач математик понимает некое общее правило, с помощью которого решение любой указанной проблемы этого класса может быть найдено чисто *механически* и «без всякой изобретательности», если, конечно, это решение существует. Среди известных примеров — *алгоритм Евклида* для нахождения

[1]) Точнее, разрешающим алгоритмом. — *Прим. перев.*

наибольшего общего делителя двух натуральных чисел или *алгоритм деления*. Алгоритм Евклида после конечного числа шагов всегда приводит к некоторому результату: он *обрывается*. Напротив, алгоритм деления обрывается только в тех случаях, когда определяемое им частное обладает конечным десятичным представлением, и только в этих случаях он приводит к определенному результату.

Интерес математиков к алгоритмам очень велик, так как алгоритмы позволяют получить — по крайней мере принципиально — схематическое решение определенного класса задач и тем самым — по крайней мере принципиально — тривиализировать определенную область математики.

Слово «алгоритм» происходит от имени арабского математика Мохаммеда ибн Муса Альхваризми, который в IX столетии внес значительный вклад в распространение существовавших тогда методов вычислений. Прогресс в развитии таких методов породил дожившее до новейших времен представление о том, что окончательным решением любой поставленной математической, и даже философской, проблемы должно быть ее алгоритмическое решение.

Среди представителей этого воззрения мы упомянем Декарта, Лейбница и Гильберта. Декарт развивал аналитическую геометрию с намерением сделать геометрию доступной алгебраическим методам вычислений и тем самым существенно продвинуться на пути к ее алгоритмизации. Лейбниц на протяжении всего своего творчества занимался уточнением и решением алгоритмических проблем. Ему же принадлежит первая попытка придумать приспособленную для этой цели *автоматически работающую машину*; правда, эта попытка не была успешной. (См. также исторические замечания в § 1 статьи «Перечислимость».) Гильберт чрезвычайно сильно стимулировал такие исследования, в особенности своими призывами к алгоритмическому решению известных классов задач (10-я проблема Гильберта, стр. 19; проблема разрешимости для так называемой логики предикатов первой ступени (см. статью «Проблема разрешимости и игра «домино»)).

2. Доказательство невозможности. Тезис Чёрча

Вера в универсальность алгоритмических методов была подорвана работой Гёделя «О формально неразрешимых предложениях principia mathematica и родственных систем» (Гёдель [3]). В этой работе была впервые доказана *алгоритмическая неразрешимость* некоторых математических проблем. Точнее, было показано, что известные математические проблемы не могут быть решены с помощью алгоритмов из некоторого точно определенного класса алгоритмов. Значение результата Гёделя зависит при этом от степени совпадения этого алгоритмического класса и класса всех алгоритмов в интуитивном смысле. Тем самым возникла совершенно новая ситуация. До тех пор, пока мы верили в возможность того, что *все* поставленные математические задачи могут быть алгоритмически решены, у нас не было повода уточнять понятие алгоритма: когда для решения какого-то класса проблем предлагался конкретный алгоритм, возникало соглашение считать указанный алгоритм действительно алгоритмом. Только утверждение об алгоритмической неразрешимости, т. е. *доказательство невозможности*, в котором содержалось бы высказывание о *всех* мыслимых алгоритмах, требует предварительного уточнения.

Начиная с 1935 г. был предложен ряд уточнений понятия алгоритма. Сегодня, за редкими исключениями (Кальмар [5], Петер [7]), господствует убеждение, что эти понятия являются адекватным выражением интуитивного представления. К этому имеются следующие основания:

a) Относительно *всех* уточнений, например, посредством *обще-рекурсивных функций* (Эрбран, Гёдель, Клини, 1934—1936), *μ-рекурсивных функций* (Гёдель, Клини, 1936), *λ-определимых функций* (Чёрч, Клини, 1933—1936), *машин Тьюринга* (Тьюринг, Пост, 1936), *марковских алгоритмов* (Марков, 1950), *графических схем* (Петер, 1958) была доказана их *эквивалентность*.

b) Все алгоритмы в *точном* смысле являются алгоритмами в *интуитивном* смысле.

c) Как показывает опыт, все известные алгоритмы могут быть «промоделированы» алгоритмами в точном смысле.

Невозможно строго доказать адекватность, так как не существует точного определения алгоритмов в интуитивном смысле. Тем не менее в настоящее время она широко используется в качестве хорошо обоснованной *гипотезы*, подобно второму началу термодинамики в физике.

Чёрч [1] первый высказал предложение, называемое ныне *тезисом Чёрча*, *отождествить* интуитивное понятие алгоритма с одним из (эквивалентных между собой) точных определений.

Мы будем следовать далее по пути, намеченному Тьюрингом [10] и Постом [8], и обоснуем понятие алгоритма, исходя из понятия *автоматически работающей машины*. Это обоснование среди прочих используемых ныне обоснований кажется с интуитивной точки зрения наиболее приспособленным для адекватного выражения понятия алгоритма. Однако предварительно необходим дальнейший анализ интуитивного представления об алгоритме.

3. Алфавиты и множества слов

Под *алфавитом* мы понимаем *конечное непустое* множество *символов*, называемых *буквами* алфавита. *Конечные* последовательности букв из некоторого алфавита A мы будем называть *словами над* A. В частности, пустая последовательность есть слово над A, так называемое *пустое слово*, которое мы будем обозначать в дальнейшем знаком $\square$. Множество слов над A мы обозначим через $\Omega(A)$, множество n-членных последовательностей слов над A — через $\Omega^n(A)$. Мы будем использовать буквы $A, \ldots$ для обозначения алфавитов, а буквы $a, \ldots, w, \ldots$ или $\mathfrak{w}, \ldots$ для обозначения соответственно элементов A, $\Omega(A)$ или $\Omega^n(A)$, где A — алфавит, о котором идет речь. Мы часто будем писать a^m $(m \geqslant 1)$ вместо $a \ldots a$ (m раз).

Множество $\Omega(A)$ является *полугруппой* с *единичным элементом* $\square$ относительно двуместной операции последовательного написания слов. Если два алфавита A и A' обладают равным числом элементов, то любое взаимно однозначное соответствие между A и A' допускает единственное продолжение до изоморфизма полугрупп $\Omega(A)$ и $\Omega(A')$.

Мы будем рассматривать в дальнейшем слова как некоторую удобную идеализацию таких объектов, которыми можно оперировать согласно определенным предписаниям (ср. п. 4). Так как предписания, относящиеся к словам над A, могут быть эффективно переведены посредством вышеупомянутого изоморфизма в предписания, относящиеся к словам над A', то без ограничения общности можно рассматривать лишь такие алфавиты, которые образованы членами некоторого непустого начального отрезка раз и навсегда заданной последовательности символов

$$\mathbf{a}_1,\ \mathbf{a}_2,\ \mathbf{a}_3,\ \ldots .$$

Мы обозначим $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ через $\mathbf{A}_n\ (n \geqslant 1)$.

Из технических соображений оказывается удобным ввести дополнительный вспомогательный символ $\mathbf{a}_0$, обозначающий *пустую*, или *несобственную*, букву. Если A — некоторый алфавит, то мы будем называть слова, образованные из $\mathbf{a}_0$ и букв A, *несобственными* словами над A. Мы будем пользоваться теми же обозначениями, что и для собственного случая. Это не приведет к путанице. Мы будем часто писать ★ вместо $\mathbf{a}_0$ и | вместо $\mathbf{a}_1$. Элементы множества $\Omega(\{|\}) = \Omega(\mathbf{A}_1) = \{\square, |, ||, \ldots\}$ будут пониматься как представления натуральных чисел; так, число $n\ (\geqslant 0)$ будет представлено n-членной последовательностью штрихов. Ввиду этого мы будем пользоваться вместо $\Omega(\mathbf{A}_1)$ более выразительным обозначением $\mathbf{N}$. Для всех допустимых алфавитов A имеем $\mathbf{N} \subset \Omega(A)$. Для натуральных чисел будут использоваться обозначения i, j, k, l, m, n, s, t.

4. Интуитивное описание понятия алгоритма

1.1. Алгоритм оперирует с конкретными, доступными воздействию (конструктивными) объектами.

Такими объектами могут быть карты при игре в скат (скажем, при осуществлении какой-либо выигрышной стратегии), костяшки счетов или теоремы какой-нибудь математической теории. Указанные объекты, если они не являются словами над некоторым алфавитом, можно *перенумеровать*, например, элементами из $\mathbf{N}$ и затем оперировать не с объектами, а с их номерами. (Полную нумерацию такого вида называют *гёделизацией.*) Таким образом, нам достаточно в дальнейшем рассматривать в качестве конструктивных объектов только слова или n-членные последовательности слов над некоторым алфавитом.

1.2. Алгоритм $\mathfrak{A}$ задается *конечным* предписанием $\mathfrak{V}$, *входным алфавитом* E, *выходным алфавитом* B, содержащим E и B *рабочим алфавитом* A и *размерным числом* n. (Мы пишем $\mathfrak{A} = \langle \mathfrak{V}, E, A, B, n \rangle$.)

Алгоритм $\mathfrak{A}$ может быть применен к n-членной последовательности $\mathfrak{w}$ слов над E. Говорят, что $\mathfrak{A}$ *применяется* к $\mathfrak{w}$, если $\mathfrak{w}$ является исходным объектом при выполнении операций, указанных в предписании $\mathfrak{V}$, с использованием букв рабочего алфавита A. Возможно, что, согласно $\mathfrak{V}$, эти операции должны быть прекращены и после этого должно быть написано слово над A; если это слово является к тому же элементом $\Omega(B)$, то оно будет *результатом* применения алгоритма. В противном случае его применение не приводит ни к какому результату. Нетрудно различить эту структуру в конкретных алгоритмах.

Мы категорически потребуем, чтобы предписание $\mathfrak{V}$ было *конечным*, т. е. чтобы определяющий его текст, написанный, например, на русском языке, был конечным. Бесконечно длинные предписания мы исключаем ввиду того, что они принципиально не допускают передачи.

Можно было бы освободиться от ограничительного требования, что алгоритмы применимы только к n-членным последовательностям слов *постоянной* длины n. Однако соответствующие обобщенные алгоритмы можно рассматривать как объединения таких алгоритмов.

Далее используются обозначения соглашения 1.2, но обсуждается для простоты только случай $n = 1$.

1.3. Предписание $\mathfrak{V}$ должно быть составлено таким образом, чтобы определяемые им операции выполнялись *поэтапно* (последовательно одна за другой).

Требование 1.3 согласуется с опытом. При реализации употребительных математических алгоритмов пробегается некоторая последовательность *позиций*, будь то позиция на счетах, состояние вычислительной машины или распределение цифр на листке с арифметическими расчетами. (Хотя на практике переход от одной позиции к другой протекает более или менее непрерывно.) Согласно этому требованию, предписание $\mathfrak{B}$ должно, помимо всего прочего, указывать, нужно ли, и если да, то каким образом, перейти от одной позиции к «следующей за ней». Часть предписания $\mathfrak{B}$, описывающую переход от одного состояния к следующему, мы назовем *указанием*.

1.4. Предписание $\mathfrak{B}$ должно быть составлено таким образом, чтобы его исполнение было *во всех деталях однозначно осуществимо* и не требовало никаких свободно принимаемых решений.

Обычные математические алгоритмы в общем не удовлетворяют требованию 1.4; однако нет никаких сомнений в том, что в каждом отдельном случае однозначность может быть достигнута уточнением предписания. Однозначность необходима, если мы хотим доверить выполнение $\mathfrak{B}$ какому-либо устройству. (При отказе от однозначности говорят, как это теперь принято, об *исчислениях* вместо алгоритмов; см. статью «Перечислимость».)

1.5. Предписание $\mathfrak{B}$ должно быть составлено таким образом, чтобы его исполнение было воспроизводимо.

Требование 1.5 должно означать следующее: применение $\mathfrak{A}$ к одному и тому же слову приводит каждый раз к реализации $\mathfrak{B}$ с одной и той же последовательностью позиций и либо ни к какому, либо к одному и тому же результату.

Требование воспроизводимости должно, в частности, исключать из рассмотрения такие предписания, в которых предусмотрено использование вычислителем какого-то вероятностного механизма, когда, например, выбор между двумя возможными операциями производится на основании результата бросания кости.

Сформулированные требования еще не исключают из общего числа «алгоритмы» такого рода:

Пусть некое устройство непрерывно бросает кость и после каждого бросания заносит в список число очков (как слова над A_1). Мы можем тогда задать с помощью детализированного предписания $\mathfrak{B}$ «алгоритм» $\mathfrak{A} = \langle \mathfrak{B}, A_1, A_1, A_1, 1 \rangle$, состоящий в следующем: пусть задано число m; просмотрим список, заполняемый этим устройством, найдем в нем число, имеющее порядковый номер m,— подождав в случае необходимости, пока устройство выпишет это число, — и объявим это число результатом.

Из интуитивных соображений мы не можем назвать процесс, определенный этим предписанием, алгоритмическим. Характерным является тот факт, что вычислитель должен пользоваться *информацией извне*, а именно: из листа, заполняемого упоминавшимся устройством. Поэтому мы введем еще следующее требование:

1.6. Предписание $\mathfrak{V}$ должно быть составлено таким образом, чтобы его исполнение не требовало информации, отличной от *содержащейся в исходном слове и в самом* $\mathfrak{V}$.

1.7. Мы не ставим *никаких* условий относительно длины $\mathfrak{V}$, длины слов, с которыми можно оперировать, и числа шагов, необходимых для исполнения $\mathfrak{V}$.

Хотя представляется вполне разумным искать основания для ограничений такого рода (исходя, например, из современных гипотез о конечности физического мира, слова произвольно большой длины не могут быть выписаны; это могут быть также ограничения экономического характера), мы хотим принять здесь *идеальную* точку зрения и отказаться от всяких ограничений.

1.8. Предписание $\mathfrak{V}$ должно быть составлено таким образом, чтобы вычислителю была необходима, возможно, сколь угодно большая, но не бесконечная память.

Мы хотим пояснить на примере, что отказ от бесконечности объема памяти вычислителя не является сколько-нибудь стеснительным. Вместо того чтобы сравнивать два слова, запоминая первое из них и сличая его «по памяти» со вторым, можно проводить это сравнение побуквенно — начиная слева — и отмечать рассматриваемые позиции внутри каждого из двух слов специальными метками. Первый способ, если предполагать его применимость к произвольной паре слов над некоторым алфавитом, требует неограниченного объема памяти, в то время как во втором случае необходимо каждый раз запоминать только метки и буквы на обоих отмеченных местах. Рассмотрение подобных примеров приводит к убеждению, что требование о неограниченной вместимости памяти можно обойти благодаря использованию подходящей системы меток. При этом метки должны каждый раз включаться в рабочий алфавит, который, конечно, должен быть достаточно большим.

Прежде чем перейти к дальнейшему анализу понятия алгоритма и выдвинуть новые условия, мотивирующие введение машин Тьюринга (§ 2), нам следует познакомиться с понятиями *вычислимой функции* и *перечислимого множества*.

5. Вычислимые функции

Мы называем функцию f *функцией из* $\Omega^n(E)$ *в* $\Omega(B)$, если область определения f, обозначаемая далее $\operatorname{Def} f$, содержится в $\Omega^n(E)$, а множество образов при отображении f, обозначаемое далее через $\operatorname{Bild} f$, содержится в $\Omega(B)$; f называется тогда также *частичной функцией на* $\Omega^n(E)$ *со значениями в* $\Omega(B)$. Если в предельном случае $\operatorname{Def} f = \Omega^n(E)$, то f называется также функцией *на* $\Omega^n(E)$ *со значениями в* $\Omega(B)$.

Алгоритм $\mathfrak{A} = \langle\mathfrak{P}, E, A, B, n\rangle$ определяет функцию $f_{\mathfrak{A}}$ из $\Omega^n(E)$ в $\Omega(B)$, если выполнены следующие требования: $f_{\mathfrak{A}}$ определена для $\mathfrak{w} \in \Omega^n(E)$ в том и только в том случае, когда применение $\mathfrak{A}$ к $\mathfrak{w}$ приводит к некоторому результату; тогда этот результат является значением $f_{\mathfrak{A}}$ от $\mathfrak{w}$. Функция $f_{\mathfrak{A}}$ обладает тем свойством, что для всех $\mathfrak{w} \in \operatorname{Def} f_{\mathfrak{A}}$ значение $f_{\mathfrak{A}}(\mathfrak{w})$ может быть *вычислено*, а именно исполнением предписания $\mathfrak{P}$. Функции с этим свойством мы называем *вычислимыми*.

1.9. Определение. Функция f из $\Omega^n(E)$ в $\Omega(B)$ называется *вычислимой* тогда и только тогда, когда существует алгоритм $\mathfrak{A} = \langle\mathfrak{P}, E, A, B, n\rangle$, для которого $f = f_{\mathfrak{A}}$; $\mathfrak{A}$ называется тогда *вычислительной процедурой* для f.

Следует отметить, что квантор существования в 1.9 следует понимать в классическом смысле; мы не требуем, чтобы для всякой вычислимой функции можно было эффективно указать соответствующую вычислительную процедуру. Пояснить это можно на таком примере:

Пусть $n = 1$, $E = B = \boldsymbol{A}_1$, и для $w \in \mathbf{N}$

$$f(w) := \begin{cases} \square, & \text{если гипотеза Римана справедлива,} \\ | & \text{в противном случае.} \end{cases}$$

Тогда f — вычислимая функция; действительно, в случае справедливости гипотезы Римана легко указать вычислительную процедуру для f. То же и в противном случае. Однако в настоящее время мы не в состоянии *эффективно* определить вычислительную процедуру для f. Предписания типа «Пишем □, если гипотеза Римана справедлива, и | в противном случае» нуждаются в использовании информации извне, а именно информации о справедливости гипотезы Римана, и в силу 1.6 являются недопустимыми.

В отличие от алгоритмов для функций возможна экстенсиональная точка зрения: две функции равны, если совпадают их области определения и если их значения во всех точках их общей области определения равны. Если в 1.9 мы *ограничим* область определения квантора существования классом точно определенных алгоритмов, содержащим для всякого алгоритма в интуитивном смысле *экстенсионально равный* ему алгоритм (два алгоритма $\mathfrak{A}$ и $\mathfrak{A}'$ экстенсионально равны, если $f_{\mathfrak{A}} = f_{\mathfrak{A}'}$, т. е. «экстенсионально равные» приблизительно означает «равные по конечному эффекту»), то мы получим то же множество вычислимых функций и одновременно *точное определение понятия вычислимой функции*. Так как мы собираемся достаточно убедительно показать, что алгоритмы, определяемые с помощью *машин Тьюринга*, образуют такой класс, то в той же степени правдоподобным станет и факт совпадения множества функций, *вычислимых по Тьюрингу* (мы определим их в § 2), с множеством функций, *вычислимых в интуитивном смысле*.

6. Разрешимость

Наряду с понятиями *вычислимой функции* и *перечислимого множества* (см. статью «Перечислимость») большую роль в алгоритмических проблемах играют также понятия *разрешимого множества* и *разрешимого отношения*. (Мы примем для отношений *экстенсиональную* точку зрения, отождествляя n-местное отношение над множеством $\mathfrak{M}$ с совокупностью тех n-членных последовательностей элементов из $\mathfrak{M}$, для которых оно выполняется. Тем самым мы оградим себя от дискуссии о *множествах*.)

Мы называем подмножество $\mathfrak{M}_1$ множества $\mathfrak{M}_2$ *конструктивных* элементов *разрешимым* относительно $\mathfrak{M}_2$, если существует алгоритм, применимый к объектам из $\mathfrak{M}_2$ и в случае применения к некоторому объекту $\mathfrak{M}_2$ дающий ответ на вопрос, принадлежит ли этот объект $\mathfrak{M}_1$.

Разрешимым является, например, множество $\mathfrak{M}_1$ уравнений, имеющих целочисленное решение, относительно множества $\mathfrak{M}_2$ всех уравнений от одного неизвестного с целыми коэффициентами. Для произвольных *диофантовых* уравнений аналогичный вопрос о разрешимости остается пока открытым (десятая проблема Гильберта)[1]).

Как и в предыдущих рассмотрениях, мы ограничимся только такими объектами, которые являются n-членными последовательностями слов над некоторым алфавитом. В такой ситуации мы можем уточнить понятие разрешимости:

1.10. Определение. Пусть $\mathfrak{M} \subset \Omega^n(E)$. Множество $\mathfrak{M}$ называется *разрешимым относительно* $\Omega^n(E)$, если существует алгоритм $\mathfrak{A} = \langle \mathfrak{B}, E, A, B, n \rangle$, применение которого к произвольному элементу $\mathfrak{w} \in \Omega^n(E)$ всегда обрывается, и результат равен $\square$ или $|$ в зависимости от того, принадлежит ли элемент $\mathfrak{w}$ множеству $\mathfrak{M}$ или нет. Такой алгоритм называется *разрешающей процедурой* для $\mathfrak{M}$ относительно $\Omega^n(E)$.

Отметим, что квантор существования в 1.10 также следует понимать в *классическом* смысле.

Следующее утверждение очевидно:

1.11. Пусть $\mathfrak{M} \subset \Omega^n(E) \cap \Omega^n(E')$. Тогда $\mathfrak{M}$ разрешимо относительно $\Omega^n(E)$ в том и только в том случае, когда $\mathfrak{M}$ разрешимо относительно $\Omega^n(E')$.

Понятие разрешимости сводится к понятию вычислимости. Точнее, имеет место такая теорема:

1.12. Теорема. *Пусть* $\mathfrak{M} \subset \Omega^n(E)$. *Множество* $\mathfrak{M}$ *разрешимо относительно* $\Omega^n(E)$ *тогда и только тогда, когда*

---

[1]) Используя результаты М. Дэвиса, Х. Путнама и Дж. Робинсон [11], [12] (1952—1961), Ю. Матиясевич [13] (1970—1971) доказал неразрешимость соответствующего множества и тем самым получил отрицательное решение 10-й проблемы Гильберта. Эти результаты интересны также в связи с вопросами перечислимости (см. далее статью Эббинхауза «Перечислимость»).—*Прим перев.*

вычислима характеристическая функция $\chi_{\mathfrak{M}}$ *множества* $\mathfrak{M}$ *относительно* $\Omega^n(E)$.

Под *характеристической функцией* $\chi_{\mathfrak{M}}$ *множества* $\mathfrak{M}$ относительно $\Omega^n(E)$ мы понимаем здесь такую функцию *на* $\Omega^n(E)$ со значениями в $\Omega(E)$, которая отображает все элементы $\mathfrak{M}$ в $\square$ и все элементы $\Omega^n(E)\setminus\mathfrak{M}$ в $|$.

Доказательство теоремы 1.12 несложно. Если $\mathfrak{M}$ разрешимо относительно $\Omega^n(E)$ и $\mathfrak{A}$ — соответствующая разрешающая процедура для $\mathfrak{M}$ относительно $\Omega^n(E)$ (без ограничения общности можно считать, что выходной алфавит $\mathfrak{A}$ есть E), то функция $\chi_{\mathfrak{M}}=f_{\mathfrak{A}}$ вычислима. Обратно, если $\chi_{\mathfrak{M}}$ вычислима и $\mathfrak{A}$ — вычислительная процедура для $\chi_{\mathfrak{M}}$, то $\mathfrak{A}$ будет и разрешающей процедурой для $\mathfrak{M}$ относительно $\Omega^n(E)$.

При предварительном обсуждении понятия разрешимости мы говорили о разрешимости множества $\mathfrak{M}_1$ относительно некоторого множества $\mathfrak{M}_2$, в определении же 1.10 рассматривался только частный случай $\mathfrak{M}_2=\Omega^n(E)$. На практике, если, скажем, $\mathfrak{M}_1\subseteq\mathfrak{M}_2\subseteq\Omega^n(E)$, а множество $\mathfrak{M}_2$ разрешимо относительно $\Omega^n(E)$, то разрешимость $\mathfrak{M}_1$ относительно $\mathfrak{M}_2$ эквивалентна разрешимости $\mathfrak{M}_1$ относительно $\Omega^n(E)$. Простое доказательство этого факта мы оставляем читателю.

§ 2. Наглядное описание и определение машины Тьюринга

1. Интуитивная стандартизация алгоритмов

Используя 1.1.—1.8, можно свести понятие алгоритма к понятию машины Тьюринга. Впервые уточнение понятия алгоритма с помощью машин Тьюринга было предпринято независимо Тьюрингом [10] и Постом [8]. Наши дальнейшие рассмотрения носят эвристический характер; мы сможем придать утверждениям лишь ограниченную степень правдоподобия, используя для этой цели примеры. Поэтому полезно проверять все утверждения на конкретных алгоритмах. Сошлемся в этой связи на работу Хермеса [4], где рассмотрен обширный круг примеров.

Обычные алгоритмы, вычисляющие с помощью слов, требуют для своего выполнения «расчетных бланков» различных форматов. Тем не менее кажется вполне правдоподобным, что произвольный алгоритм может быть промоделирован алгоритмом, использующим *счетную ленту*, разделенную на ячейки и ограниченную слева, но не ограниченную справа:

Поскольку, согласно 1.7, мы отказались от ограниченности длин слова, мы вынуждены хотя бы в принципе допустить такого рода неограниченность. Подобным образом кажется несущественным требование, чтобы одна ячейка ленты заполнялась *не более чем одной* буквой. Существенным является требование—оно мотивировано условием 1.1,—что записи имеются лишь *в конечном числе ячеек*. Мы договоримся на будущее считать пустую ячейку содержащей *пустую* букву a_0. Таким образом, почти все ячейки будут содержать a_0.

Согласно 1.3, выполнение алгоритма является поэтапным, и если оно не обрывается, всегда ведет от одного состояния к другому. Предписание для алгоритма наряду с общими правилами, определяющими, как должен быть выделен результат после окончания вычислений и т. п., содержит последовательность *указаний* относительно перехода от одного состояния к другому, непосредственно за ним следующему (согласно 1.4 и 1.5, этот переход определен однозначно). Каждое указание требует от вычислителя при заданном состоянии определенного *образа действий*. Мы руководствуемся здесь наглядным представлением о том, что действия вычислителя могут включать в себя *изменение содержимого отдельной ячейки ленты*, *поиск другой ячейки ленты* или *прекращение вычислений*. Во втором случае мы можем ограничиться только выбором одной из *соседних* ячеек; вопрос о перескакивании через несколько ячеек будет таким образом разрешен. Ячейку, с которой оперирует вычислитель в некоторый момент времени, мы назовем *текущей рабочей ячейкой*. Можно на примерах убедиться в том, что после соответствующего уточнения предписания изменение записи на ленте будет всегда происходить только в рабочей ячейке. Таким образом, для любого состояния предписываемый некоторым указанием образ действий вычислителя может состоять лишь в следующем: *изменить содержимое рабочей ячейки*, *сдвинуть рабочую ячейку на одну ячейку вправо* или (если это возможно) *влево*, *остановиться*. Согласно требованиям 1.4—1.6, порядок действий должен быть указан однозначно и вполне ясно. Если процесс не остановлен, указание должно точно предписывать, к какому другому указанию следует переходить непосредственно вслед за этим.

И наконец, осталось выяснить, какие факторы влияют на порядок действий, определяемый данным указанием в некотором состоянии. Согласно 1.6, мы можем допустить, что для оценки текущего состояния, предваряющей выполнение некоторого указания, могут быть привлечены только *текущая запись на ленте*, *текущая рабочая ячейка* и *история* проведения вычислений. Мы обратимся сначала к первым двум характеристикам.

Следуя 1.8, мы можем предполагать наличие у вычислителя лишь *ограниченной* памяти. Для оценки состояния может поэтому привлекаться только *ограниченная* часть записей на ленте. Ввиду того что просмотр записи, содержащей не более k ячеек, может быть осуществлен в виде k-кратного просмотра содержимого только одной ячейки за раз, кажется интуитивно оправданным предположение о том, что для оценки текущего состояния необходимо чтение содержимого лишь одной-единственной ячейки, которую мы назовем *текущей информационной ячейкой*. Далее, разумно считать, что рабочая и информационная ячейки совпадают. Действительно, в противном случае можно изменить предписание таким образом, чтобы сначала рабочая ячейка сменялась информационной и чтобы далее, с учетом содержимого этой последней ячейки, разыскивалась исходная рабочая ячейка и определялся требуемый порядок действий.

Таким образом, при оценке состояния с целью получения соответствующего указания используются только рабочая ячейка, ее содержимое и исторические сведения о ходе предыдущих вычислений. Ссылка на историю может быть, однако, устранена. Следующий сравнительно простой пример показывает, как можно избежать такой ссылки.

Пусть рабочий алфавит есть A_1. Предписание $\mathfrak{B}$ содержит k ($\geqslant 3$) указаний. В частности, первое указание предписания $\mathfrak{B}$ гласит:

если рабочая ячейка содержит a_0, остановись;
если рабочая ячейка содержит $|$, замени $|$ буквой a_0 и действуй далее согласно второму указанию.

Второе указание:

если рабочая ячейка содержит a_0, замени a_0 буквой $|$ в том случае, *когда предыдущее действие выполнялось согласно первому указанию*, и действуй далее согласно третьему указанию; в противном случае остановись;
если рабочая ячейка содержит $|$, остановись.

Выделенная курсивом ссылка во втором указании может быть устранена, например, так. Мы введем ($k+1$)-е указание:

если рабочая ячейка содержит a_0, замени a_0 на $|$ и действуй далее согласно третьему указанию;
если рабочая ячейка содержит $|$, остановись.

Затем мы заменим во второй части первого указания слово «второму» словом «($k+1$)-му» и перепишем второе указание таким образом:

если рабочая ячейка содержит a_0, остановись;
если рабочая ячейка содержит $|$, остановись.

Измененное таким образом предписание совпадает по своему действию с исходным, но не содержит ссылок. Влияние, оказываемое прошлым вычислительного процесса на его будущее, больше не нуждается в *явном* выражении: оно определяется *положением* (т. е. порядковым номером, если предполагать наличие такой нумерации) внутри предписания того указания, согласно которому проводятся вычисления в данный момент.

Исходя из этого, мы можем считать достаточно правдоподобным следующее утверждение:

2.0. Каждому алгоритму соответствует экстенсионально эквивалентный ему алгоритм, работающий с уже упоминавшейся лентой и обладающий следующими особенностями. В каждый момент реализации алгоритма его рабочее состояние определяется текущей рабочей ячейкой и ее содержимым в тот же момент; общая ситуация для всего вычислительного процесса вплоть до данного момента полностью определяется текущей рабочей ячейкой, текущим содержимым всей ленты и тем указанием (или его номером), согласно которому проводятся текущие вычисления. Отдельные указания требуют от вычислителя выполнения одного из следующих типов действий, выбор которого определяется полностью и однозначно содержимым рабочей ячейки: изменение содержимого рабочей ячейки, сдвиг рабочей ячейки на одну ячейку вправо или (если возможно) влево, останов. В первых двух случаях указание определяет, к выполнению какого следующего указания нужно перейти.

2. Машины Тьюринга

Алгоритмы, указания которых имеют описанную выше стандартную форму, могут быть непосредственно промоделированы на машинах Тьюринга. Ввиду 2.1 вполне правдоподобно, что такие машины — после введения предписаний общего характера — явятся адекватным уточнением понятия алгоритма. Так как эти общие предписания, которые касаются задания n-членной последовательности слов, выделения возможных результатов и тому подобных вещей, сами по себе не представляют теоретических трудностей, то мы определим их в соответствующем месте сразу для машин Тьюринга. Мы хотели бы отметить, что наряду с рассматриваемым нами типом машин в литературе встречается целый ряд эквивалентных между собой вариантов. Так, например, в работе Хермеса [4] в основу положен тип машин, в которых счетная лента не ограничена с обеих сторон.

Машина Тьюринга (сокращенно м. Т.) T в главных чертах состоит из *операционного исполнительного устройства*, которое может находиться в одном из дискретных *состояний* $q_0, \ldots, q_s$, принадлежащих некоторой конечной совокупности, комбинированной *читающей и пишущей головки*, *счетной ленты*, описанной в предыдущем пункте, и *лентопротяжного механизма*. При этом q_0 называется начальным состоянием T. Ячейки ленты пронумерованы, начиная с крайней левой, числами 0, 1, 2, ... Читающая и пишущая головка находится в каждый данный момент времени над некоторой ячейкой ленты—текущей *рабочей ячейкой*. С помощью лентопротяжного механизма одна из ячеек, соседняя с рабочей ячейкой, может быть помещена под читающей и пишущей головкой; в таком случае мы будем говорить, что *рабочая ячейка сдвинулась на одну ячейку вправо или влево*.

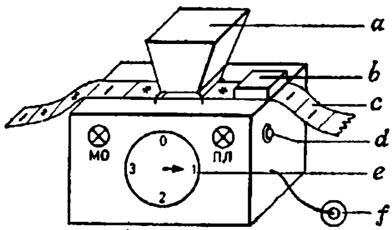


Рис. 1.

a—читающая и пишущая головка, b—лентопротяжный механизм, c—лента, d—пусковая кнопка, e—указатель состояния, f—источник энергии.

Читающая и пишущая головка может читать буквы алфавита $A = \{a_1, \ldots, a_t\}$ и букву a_0, стирать их и печатать; A называется *рабочим алфавитом* T. Каждая ячейка ленты в каждый момент содержит букву из множества $A \cup \{a_0\}$, при этом почти все ячейки заняты буквой a_0. Наглядное представление о машине Тьюринга дает рис. 1.

Лампа МО зажигается при выполнении указания об остановке («Машинный останов»; см. ниже), лампа ПЛ зажигается, когда остановка вызвана тем, что начальная ячейка ленты находится под считывающей головкой, а требуемое действие состоит в сдвиге рабочей ячейки влево («Переход за край ленты»; см. ниже).

Прежде чем мы опишем характер работы м.Т. в общем случае, рассмотрим работу некоторой конкретной м.Т. T с рабочим алфавитом $\{|\}$ и тремя рабочими состояниями q_0, q_1, q_2. Работа T может быть описана следующим образом.

Порядок действий в состоянии q_0: независимо от содержимого рабочей ячейки (т. е. от того, стоит ли в рабочей ячейке знак ★ или |) T сдвигает рабочую ячейку вправо и переходит в состояние q_1.

Порядок действий в состоянии q_1: T заменяет букву, стоящую в рабочей ячейке (т. е. ★ или |), буквой | и переходит в состояние q_2.

Порядок действий в состоянии q_2: T останавливается независимо от содержимого рабочей ячейки.

Очевидно, что T делает следующее: после установки головки над некоторой ячейкой ленты (состояние q_0) T сдвигает рабочую ячейку вправо, стирает содержимое этой ячейки, заносит туда знак | и останавливается.

Позже мы будем описывать порядок работы T следующей матрицей, так называемой таблицей T (отметим, что символ q_2, стоящий в конце двух последних строчек, не играет никакой роли):

q_0	★	r	q_1
q_0	|	r	q_1
q_1	★	|	q_2
q_1	|	|	q_2
q_2	★	s	q_2
q_2	|	s	q_2

Мы рассмотрим работу T на примере с помощью серии рисунков (рис. 2—7). Для этого мы выберем начальную ячейку ленты в качестве рабочей ячейки и допустим, что

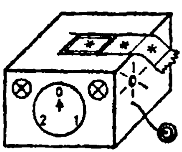


Рис. 2

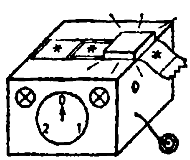


Рис. 3

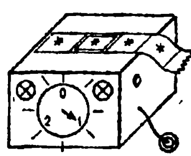


Рис. 4

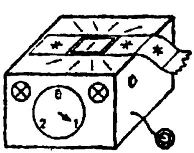


Рис. 5

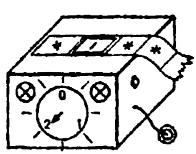


Рис. 6

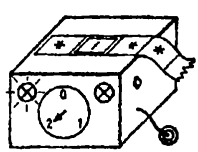


Рис. 7

лента содержит только пустые буквы. Мы отказались от изображения на рисунках читающей и пишущей головки и лентопротяжного механизма (кроме рис. 3), рабочую ячейку мы выделили специальной рамкой.

Пуск T происходит в состоянии q_0 (рис. 2), далее T обнаруживает ★ в рабочей ячейке, сдвигает ввиду этого рабочую ячейку на одну ячейку вправо (рис. 3) и переходит в состояние q_1 (рис. 4). Затем T заменяет знак ★, находящийся в текущей рабочей ячейке, знаком | (рис. 5) и переходит в состоянии q_2 (рис. 6). В этой ситуации T должна прекращать работу, поэтому она останавливается и зажигается лампа МО (рис. 7).

После этих приготовлений мы можем дать теперь общее описание.

Порядок работы м.Т. T (с рабочим алфавитом $A = \boldsymbol{A}_t$ и состояниями $q_0, \ldots, q_s$) описывается *таблицей* машины T. Эта таблица есть матрица с 4 столбцами и $(s+1)(t+1)$ строками; строка матрицы с номером $(j(t+1)+k+1)$ $(0 \leqslant j \leqslant s,\ 0 \leqslant k \leqslant t)$ имеет вид

$$q_j a_k v_{jk} q_{jk},$$

где $v_{jk} \in A \cup \{a_0, \boldsymbol{r}, \boldsymbol{l}, \boldsymbol{s}\}$, $q_{jk} \in \{q_0, \ldots, q_s\}$. Здесь $\boldsymbol{r}, \boldsymbol{l}, \boldsymbol{s}$ — новые символы. Мы назовем для данной строки v_{jk} *действием*, а q_{jk} — *следующим состоянием*. Для строки таблицы мы будем пользоваться сокращенным обозначением $qavq'$ и, в частности, $qaa'q'$, $qa\boldsymbol{r}q'$ или $qa\boldsymbol{l}q'$, если действие есть буква из $A \cup \{a_0\}$, $\boldsymbol{r}$ или $\boldsymbol{l}$ соответственно.

Итак, T работает согласно следующим правилам: если T находится в состоянии q, читающая и пишущая головка сначала прочитывает содержимое a рабочей ячейки. Пусть $qavq'$ есть (единственная) строка таблицы T, начинающаяся парой символов qa. Если $v \in A \cup \{a_0\}$, то читающая и пишущая головка стирает содержимое рабочей ячейки и заносит туда букву v. Если $v = \boldsymbol{r}$, то рабочая ячейка сдвигается на одну ячейку вправо. Если $v = \boldsymbol{l}$ и рабочая ячейка не совпадает с нулевой ячейкой, то рабочая ячейка сдвигается на одну ячейку влево.

Во всех этих случаях T переходит в конце концов в следующее состояние q' и процесс соответствующим образом повторяется. Если $v = \boldsymbol{l}$, а рабочая ячейка есть нулевая ячейка, то требуемое действие невыполнимо: тогда

T *останавливается*. В этом случае мы говорим, что T *вышла за пределы ленты*. Если, наконец, $v = \mathbf{s}$, то T точно так же *останавливается*, и мы говорим, что произошел *машинный останов* T. Мы употребляем слово *останов* как профессионально-жаргонный вариант слова остановка.

Каждая часть таблицы T, состоящая из строк с одинаковым начальным символом q, соответствует, очевидно, некоторому указанию в том смысле, в каком это понятие разъяснялось в п. 1; при этом состояния T отвечают номерам указаний в соответствующем алгоритмическом предписании.

В дальнейшем мы не будем строго различать м.Т. и ее таблицу. Таблицы удобны для различных конструкций; они будут выступать на передний план, когда мы будем рассматривать машины Тьюринга как конструируемые объекты (таблице T отвечает тогда машина $M(T)$).

Мы понимаем запись на ленте (или, короче, *запись*) как функцию $\mathfrak{I}$ на $\mathbf{N}$ со значениями в $A \cup \{a_0\}$, которая каждому i сопоставляет букву, являющуюся содержимым i-й ячейки ленты. Неравенство $\mathfrak{I}(i) \neq \bigstar$ выполняется лишь для конечного числа индексов i.

Как было принято для описанных в п. 1 алгоритмов, общий итог выполненных вычислений однозначно определен тройкой $(m, \mathfrak{I}, q)$, где m есть номер текущей рабочей ячейки, $\mathfrak{I}$ — текущая запись и q — текущее состояние T. Мы назовем такую тройку *конфигурацией* машины T. В качестве обозначений для конфигураций используются буквы $C, \ldots$. *Начальными конфигурациями* называются конфигурации, третья компонента которых есть q_0.

Пусть $C = (m, \mathfrak{I}, q)$ — некоторая конфигурация T. Если $q\mathfrak{I}(m)vq'$ есть строка таблицы T, начинающаяся символами $q\mathfrak{I}(m)$, и если $v \neq \mathbf{s}$ и не выполняются одновременно равенства $v = \mathbf{l}$ и $m = 0$, то выполнение действия v приводит к новой рабочей ячейке с номером m' (при этом, конечно, возможно равенство $m = m'$) и к новой записи $\mathfrak{I}'$ (при этом, конечно, возможно равенство $\mathfrak{I} = \mathfrak{I}'$) и T переходит в состояние q'. Однозначно определенную конфигурацию $C' = (m', \mathfrak{I}', q')$ мы называем *конфигурацией, следующей за* C. Наоборот, если $v = \mathbf{s}$ или $v = \mathbf{l}$ и $m = 0$, то конфигурации, следующей за C, не существует. Мы назовем в этом случае C *конечной конфигурацией* (для T).

Говорят, что T *применяется к записи* $\mathfrak{I}$ *в рабочей ячейке* m, если в качестве начальной конфигурации выбрана конфигурация $C_0=(m, \mathfrak{I}_0, q_0)$. Конфигурация C_0 однозначным образом порождает конечную или бесконечную *последовательность конфигураций* $C_0, C_1, C_2, \dots$, в которой всегда C_{i+1} есть конфигурация, следующая за C_i, и для которой C_i есть последний член в том и только в том случае, когда C_i является конечной конфигурацией. В согласии с представлением о том, что работа T состоит в последовательном выполнении отдельных шагов, мы назовем C_i *конфигурацией после i-го шага*. В частности, C_0 есть конфигурация после нулевого шага. Если C_i и C_{i+1} — члены указанной последовательности, то мы говорим, что *на* $(i+1)$*-ом шаге* T *переходит от* C_i *к* C_{i+1}. Если C_i есть последний член этой последовательности, то мы скажем, что *после i-го шага* T *остановилась*.

Говорят, что T *остановилась через конечное число шагов после применения к записи* $\mathfrak{I}$ *в рабочей ячейке* m, если последовательность конфигураций, порожденная $C_0 = (m, \mathfrak{I}, q_0)$, имеет последний член.

Каждой конфигурации $C=(m, \mathfrak{I}, q)$ мы сопоставляем ее *позицию* $S=(m, \mathfrak{I})$. Позиции — мы будем обозначать их буквами $S, \dots$ — служат удобным средством описания процесса вычислений, если не интересоваться состояниями. Последовательности конфигураций соответствует *последовательность позиций*. На них переносится почти буквально терминология, принятая для последовательностей конфигураций. В частности, говорят, что *начальной позицией* выбрана позиция $S=(m, \mathfrak{I})$, если начальная конфигурация есть $(m, \mathfrak{I}, q_0)$. *Конечной позицией* после выполнения вычислений будет позиция, сопоставляемая соответствующей конечной конфигурации.

Пусть $C=(m, \mathfrak{I}, q)$ есть некоторая конфигурация и $\mathfrak{I}(i)=a_i$ для всех $i \geqslant 0$. Мы введем обозначения

$$a_0 \dots a_m^q \dots \quad \text{и} \quad a_0 \dots \underset{\uparrow}{a_m} \dots$$

для наглядного изображения C и (соответственно) связанной с C позиции. Когда потребуется, мы будем часто изменять такой порядок записи, причем это всегда можно будет легко заметить. Безразличные для нас связные куски записи мы будем часто изображать знаком $\sim$, а если речь идет о содержимом одной-единственной ячейки, то знаком $-$.

Для записи позиций мы примем следующие соглашения:

a) Разрешается в отдельных случаях изображать только интересующую нас часть записи. Пример: $\bigstar \sim | \underset{\uparrow}{-} \bigstar$.

b) Если (левый) край ленты играет в записи какую-то роль, то мы обозначаем его знаком $]$. Пример: $] \bigstar \bigstar \underset{\uparrow}{|} \bigstar |$.

c) Символы $\bigstar \ldots$ в конце записи означают, что все правее лежащие ячейки содержат букву $\bigstar$. Пример: $] \bigstar | \underset{\uparrow}{\bigstar} \ldots$.

Мы думаем, что ввиду наглядного характера такого способа записи точное определение будет излишним.

Пусть S и S' — возможные позиции для T; мы будем писать

$$S \overset{T}{\Longrightarrow} S',$$

если S является начальной позицией для T и при этом T останавливается после конечного числа шагов в конечной позиции S'. Пример:

$$] \bigstar w \underset{\uparrow}{\bigstar} \ldots \overset{T}{\Longrightarrow}] - \bigstar | \underset{\uparrow}{\bigstar}.$$

Для удобства определения функций, вычислимых по Тьюрингу, мы примем еще несколько терминологических соглашений.

Применить T к записи после слова w или после n-членной последовательности слов $(w_1, \ldots, w_n)$ *над A* означает взять в качестве начальной следующую позицию:

$$] \bigstar w \underset{\uparrow}{\bigstar} \ldots, \text{ соответственно }] \bigstar w_1 \bigstar \ldots \bigstar w_n \underset{\uparrow}{\bigstar} \ldots.$$

Применить T к записи перед словом w или перед n-членной последовательностью слов $(w_1, \ldots, w_n)$ *над A* означает взять в качестве начальной следующую позицию:

$$] \underset{\uparrow}{\bigstar} w \bigstar \ldots, \text{ соответственно }] \underset{\uparrow}{\bigstar} w_1 \bigstar \ldots \bigstar w_n \bigstar \ldots.$$

Применить T к пустой ленте означает взять в качестве начальной позицию

$$] \underset{\uparrow}{\bigstar} \ldots.$$

Пусть w — некоторое слово над A. Будем говорить, что T *остановилась после*, соответственно *перед словом* w, если T применялась к начальной записи $\mathfrak{I}$ в начальной рабочей ячейке ($S = (m, \mathfrak{I})$) и

$$S \overset{T}{\Longrightarrow} \mathbf{|} \sim \bigstar w \underset{\uparrow}{\bigstar}, \text{ соответственно } S \overset{T}{\Longrightarrow} \mathbf{|} \sim \underset{\uparrow}{\bigstar} w \bigstar.$$

(В конечной позиции о содержимом ячеек, находящихся правее последнего символа $\bigstar$, ничего нельзя сказать.)

Если T в результате применения к записи $\mathfrak{I}$ в рабочей ячейке m остановилась *после* слова w над A, то последняя рабочая ячейка, даже если $w = \square$, не может быть нулевой ячейкой; таким образом, произошел *машинный останов* T,

3. Функции, вычислимые по Тьюрингу

Пусть T есть м.Т. с рабочим алфавитом A. Пусть $E, B \subset A$ и $n \geqslant 0$. Тогда T *определяет некоторую n-местную функцию f из $\Omega^n(E)$ в $\Omega(B)$* по следующему правилу: $\mathfrak{w} \in \Omega^n(E)$ принадлежит области $\mathrm{Def}\, f$ тогда и только тогда, когда T, примененная к записи после $\mathfrak{w}$, останавливается после слова из $\Omega(B)$; это слово является значением f от $\mathfrak{w}$. Таким образом, для $(w_1, \ldots, w_n) \in \Omega^n(E)$ имеем

$$\mathbf{|} \bigstar w_1 \bigstar \ldots \bigstar w_n \underset{\uparrow}{\bigstar} \ldots \overset{T}{\Longrightarrow} \mathbf{|} \sim \bigstar f(w_1, \ldots, w_n) \underset{\uparrow}{\bigstar},$$

когда $(w_1, \ldots, w_n) \in \mathrm{Def}\, f$. Наоборот, если $(w_1, \ldots, w_n) \notin \mathrm{Def}\, f$, то T, примененная к записи после $(w_1, \ldots, w_n)$, *не останавливается после слова из* $\Omega(B)$.

В согласии с 1.9 мы дадим для всех $n \geqslant 0$ такое определение:

2.1. Определение. Функция f из $\Omega^n(E)$ в $\Omega(B)$ называется *вычислимой по Тьюрингу* (сокращенно в.Т.), если существует м.Т. с рабочим алфавитом A, содержащим E и B, такая, что n-местная функция из $\Omega^n(E)$ в $\Omega(B)$, определяемая машиной T, совпадает с f. О любой такой м.Т. T говорят, что она *вычисляет* f.

Мы подчеркиваем, что так же, как и в 1.9, квантор существования в 2.1 следует понимать в *классическом* смысле. Если f есть в. Т. функция из $\Omega^n(E)$ в $\Omega(B)$ и T есть м.Т., вычисляющая f, то наглядное истолкование 2.1 таково: применим T к $\mathfrak{w} \in \Omega^n(E)$; тогда либо T не остановится вовсе, либо T уйдет за пределы ленты, либо произойдет машинный останов T. Если в последнем случае T остановилась после слова w и если $w \in \Omega(B)$, то $\mathfrak{w} \in \mathrm{Def}\, f$ и $f(\mathfrak{w}) = w$. Во всех остальных случаях $\mathfrak{w} \notin \mathrm{Def}\, f$.

Описание применения T к аргументу в. Т. функции, вычисляемой T, и определение значения функции способом, указанным в 2.1, образуют вместе *общее предписание*. Тем самым полностью закончено описание алгоритмов. Согласно вводным замечаниям п.2, представляется достаточно убедительным, что *понятие в. Т. функции является адекватной формализацией интуитивного понятия вычислимой функции.*

Позже мы часто будем использовать технически важное понятие *нормированно* вычислимой по Тьюрингу функции:

2.2. Определение. Функция f из $\Omega^n(E)$ в $\Omega(B)$ называется *нормированно* в. Т. функцией, если существует м.Т. T, которая вычисляет f и при этом удовлетворяет следующим требованиям: если $\mathfrak{w} \in \Omega^n(E)$ и $\mathfrak{w} \notin \mathrm{Def}\, f$, то T никогда не останавливается после применения к $\mathfrak{w}$; если же $\mathfrak{w} \in \mathrm{Def}\, f$ и $\mathfrak{w} = (w_1, \ldots, w_n)$, то

$$\underset{}{|} \star w_1 \star \ldots \star w_n \underset{\uparrow}{\star} \ldots \overset{T}{\Longrightarrow}$$

$$\overset{T}{\Longrightarrow} | \star w_1 \star \ldots \star w_n \star f(w_1, \ldots, w_n) \underset{\uparrow}{\star} \ldots .$$

О любой такой м. Т. T мы скажем, что она осуществляет *нормированное* вычисление f.

Каждая нормированно в. Т. функция является в. Т. функцией. Обращение этого утверждения будет доказано в § 4 следующей статьи.

Значение нормированного вычисления заключается в следующем. Если T осуществляет нормированное вычисление функции f из $\Omega^n(E)$ в $\Omega(B)$, то после применения T к записи

$$| \sim \star w_1 \star \ldots \star w_n \underset{\uparrow}{\star} \ldots$$

при $\mathfrak{w} = (w_1, \ldots, w_n) \in \Omega^n(E) \setminus \mathrm{Def}\, f$ машина T не останавливается, и, наоборот, при $\mathfrak{w} \in \mathrm{Def}\, f$ машина T реализует вывод:

$$\rbrack \sim \bigstar w_1 \bigstar \ldots \bigstar w_n \underset{\uparrow}{\bigstar} \ldots \overset{T}{\Longrightarrow}$$

$$\overset{T}{\Longrightarrow} \rbrack \sim \bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar f(\mathfrak{w}) \underset{\uparrow}{\bigstar} \ldots,$$

не переходя при этом за левую звездочку. Содержимое части $\sim$ счетной ленты не влияет на работу T и в ходе вычислений не меняется.

МАШИНЫ ТЬЮРИНГА И ВЫЧИСЛИМЫЕ ФУНКЦИИ II

Ф. К. МАН

Это вторая часть вводной статьи о машинах Тьюринга (м. Т.) и вычислимых функциях. Первая и третья части, написанные Г.-Д. Эббинхаузом, также находятся в этой книжке; единства ради мы проводим сплошную нумерацию параграфов во всех трех частях статьи.

В § 3 этой части описаны простые примеры машин Тьюринга и развит метод их представления посредством блок-схем. В § 4 будет показано, что для любой вычислимой по Тьюрингу функции существует машина Тьюринга, которая осуществляет нормированное вычисление этой функции без использования вспомогательных букв; и в заключение в § 5 будут рассмотрены простые примеры неразрешимых множеств.

Для понимания этой части статьи достаточно знакомства с первой частью.

§ 3. *Примеры машин Тьюринга. Диаграммы Тьюринга*

Для начала мы опишем здесь несколько простых м.Т., которые понадобятся нам и в дальнейшем.

1. Элементарные машины

Элементарные машины — это м. Т. с рабочим алфавитом A_t. Результатом их применения к произвольной позиции являются некоторые «элементарные» изменения.

а) М.Т. a_i $(0 \leqslant i \leqslant t)$, примененная к произвольной позиции, печатает в рабочей ячейке букву a_i и останавливается на этой ячейке, не изменяя других записей. Очевидно, что так работает м. Т. с таблицей

$$\begin{array}{cccc} q_0 & a_0 & a_i & q_1 \\ & & \vdots & \\ q_0 & a_t & a_i & q_1 \\ q_1 & a_0 & s & q_1 \\ & & \vdots & \\ q_1 & a_t & s & q_1 \end{array}$$

Итак, на первом шаге в рабочую ячейку независимо от ее содержимого заносится буква a_i, и после этого шага машина останавливается.

b) М.Т. r, примененная к произвольной позиции, сдвигает рабочую ячейку на одну ячейку *вправо* и затем останавливается, не изменяя записи на ленте. Так работает м.Т. с таблицей

$$\begin{array}{cccc} q_0 & a_0 & r & q_1 \\ & & \vdots & \\ q_0 & a_t & r & q_1 \\ q_1 & a_0 & s & q_1 \\ & & \vdots & \\ q_1 & a_t & s & q_1 \end{array}$$

c) М.Т. l, примененная к произвольной позиции, сдвигает рабочую ячейку на одну ячейку *влево* и затем останавливается, не изменяя записи на ленте. Это указание не всегда выполнимо (а именно, оно невыполнимо в случае, когда рабочая ячейка имеет нулевой номер). В этом случае мы потребуем, чтобы в результате ухода за пределы ленты машина останавливалась на нулевой ячейке, не меняя записи на ленте. Так работает м.Т. с таблицей

$$\begin{array}{cccc} q_0 & a_0 & l & q_1 \\ & & \vdots & \\ q_0 & a_t & l & q_1 \\ q_1 & a_0 & s & q_1 \\ & & \vdots & \\ q_1 & a_t & s & q_1 \end{array}$$

2. Другие машины

а) Машина, которая независимо от начальной позиции сдвигает рабочую ячейку на три ячейки вправо, печатает там букву a_0 и останавливается, не внося в запись других изменений. Так работает м. Т. с таблицей

$$
\begin{array}{cccc}
q_0 & a_0 & r & q_1 \\
 & & \vdots & \\
q_0 & a_t & r & q_1 \\
q_1 & a_0 & r & q_2 \\
 & & \vdots & \\
q_1 & a_t & r & q_2 \\
q_2 & a_0 & r & q_3 \\
 & & \vdots & \\
q_2 & a_t & r & q_3 \\
q_3 & a_0 & a_0 & q_4 \\
 & & \vdots & \\
q_3 & a_t & a_0 & q_4 \\
q_4 & a_0 & s & q_4 \\
 & & \vdots & \\
q_4 & a_t & s & q_4
\end{array}
$$

b) М. Т., переводящая начальную позицию

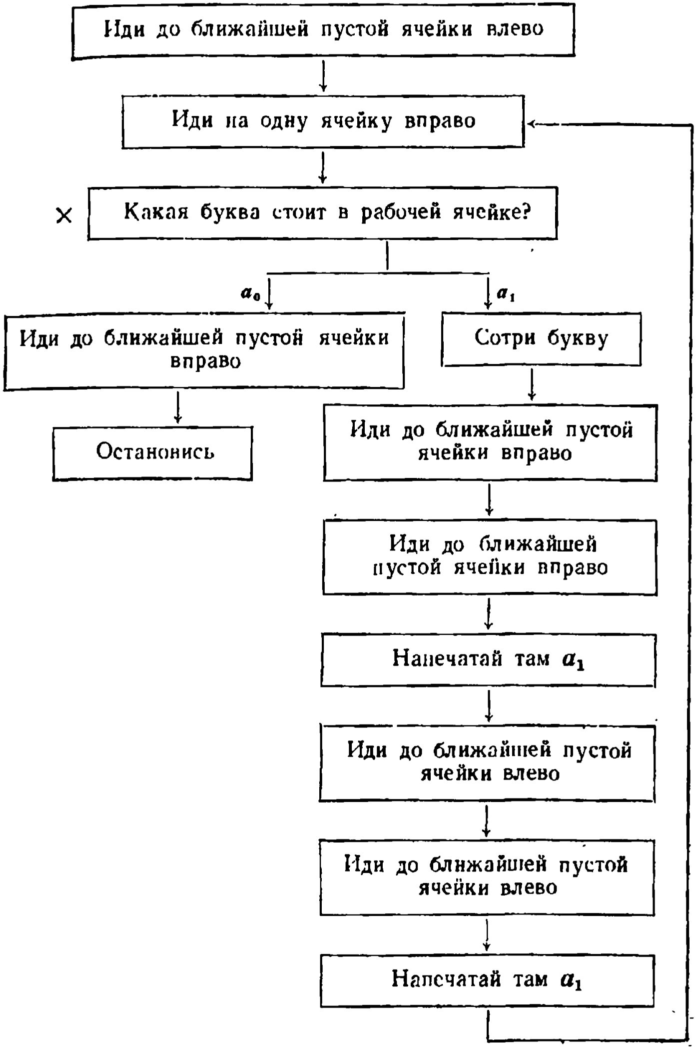
$$\sim \bigstar w \underset{\uparrow}{\bigstar} \ldots$$

в конечную позицию

$$\sim \bigstar w \bigstar w \underset{\uparrow}{\bigstar} \ldots .$$

При этом м. Т. не должна во время работы выходить на сегмент записи, обозначенный $\sim$, и, в частности, не должна его изменять. Простоты ради мы выберем в качестве входного и рабочего алфавитов алфавит A_1 (м. Т. такого же действия с входным и рабочим алфавитом A_t описана в п. 8).

Для описания работы такой машины целесообразно составить сначала «блок-схему», как это делается обычно при описании программ для электронных вычислительных устройств.



(Поясним порядок работы: w копируется буква за буквой, и машина «отмечает», какую букву w она копирует в данный момент, для чего эта буква стирается, а после того как она скопирована, возобновляется. Окончание копирования машина «замечает», когда на вопрос, стоящий в отмеченной крестиком рамке, она получает ответ «a_0» действительно, она находится в этот момент в ячейке непосредственно после w.)

Из этой блок-схемы ясно, что нужные действия выполняет м. Т. с таблицей

$q_0 \bigstar l q_1$	$q_4 \bigstar r q_5$	$q_8 \bigstar \mid q_2$
$q_0 \mid l q_1$	$q_4 \mid l q_1$	$q_8 \mid l q_8$
$q_1 \bigstar \bigstar q_2$	$q_5 \bigstar r q_6$	$q_9 \bigstar s q_9$
$q_1 \mid l q_1$	$q_5 \mid r q_5$	$q_9 \mid r q_9$
$q_2 \bigstar r q_3$	$q_6 \bigstar \mid q_7$	
$q_2 \mid r q_3$	$q_6 \mid r q_6$	
$q_3 \bigstar r q_9$	$q_7 \bigstar l q_8$	
$q_3 \mid \bigstar q_4$	$q_7 \mid l q_7$	

3. Зачем нужны диаграммы Тьюринга?

Из примеров п. 2 видно, что для выполнения даже простых задач нужны очень сложные м. Т. Было бы желательно иметь некоторый общий метод, позволяющий «собирать» м. Т. В примере a), скажем, мы могли бы поместить одну за другой три машины r и одну машину a_0; в примере b) мы могли бы сначала сконструировать машины для частных задач и затем собрать из них нужную машину.

Из примера b) видно также, что наряду с простым соединением машин (когда машина M' должна работать независимо от того, какая буква стояла в последней рабочей ячейке перед машинным остановом M) была бы желательна возможность и их дифференцированного соединения (т. е. такого, что если в последней рабочей ячейке перед машинным остановом M стояла буква a_0, то дальше должна работать машина $M'_0, \ldots$, если там стояла буква a_l, — то машина M'_l). Простое соединение может рассматриваться как частный случай дифференцированного соединения.

4. Определение диаграммы Тьюринга

Сказанное в п. 3 оправдывает следующее определение. Пусть символы $M_1, \ldots, M_n$ обозначают данные м.Т., имеющие общий рабочий алфавит A_t. С помощью этих символов, а также отличного от них символа $\cdot$ (точка) можно составить диаграмму Тьюринга D, выписав некоторые из этих символов (возможно, неоднократно) и соединив их между собой стрелками с надписанными на них буквами. При этом мы потребуем, чтобы

(i) символ $\cdot$ (точка) встречался в D только один раз (он должен указывать, где нужно начинать работу);

(ii) из любого символа для каждого $j = 0, \ldots, t$ выходило не более одной стрелки с буквой a_j (должно быть однозначно определено, какая машина должна работать следующей, после того как имел место машинный останов некоторой другой машины при условии, что в ее последней рабочей ячейке стояло a_j).

Отметим, что стрелка может вести и от символа к нему самому.

5. Разъяснение порядка работы машины T, заданной некоторой диаграммой

Пусть T применяется к некоторой определенной позиции. Пусть рабочая ячейка содержит букву a. Если из точки не выходит стрелка с буквой a, то машина T производит машинный останов. Наоборот, если из точки выходит стрелка с буквой a, то, согласно (ii), может быть только одна такая стрелка. Она ведет либо к символу M_i, либо в точку. Второй случай неинтересен; мы можем, например, потребовать, чтобы такая машина, не изменяя позиции, продолжала работать дальше и тем самым никогда не останавливалась. В первом случае T должна начать работать, как M_i, с той же начальной позицией: T переходит за край ленты, если это делает M_i; T не останавливается, если не останавливается M_i, и при этом последовательно проходит те же позиции, что и M_i. Если, наоборот, в ходе вычислений на M_i имел место машинный останов, то T должна установить, какая буква содержится в текущей рабочей ячейке. Если в диаграмме нет выходящей из M_i

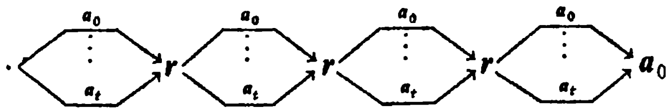
стрелки с этой буквой, то должен иметь место машинный останов T. Если же из M_i выходит такая стрелка, то T должна работать дальше, как машина, которая находится на конце этой стрелки и начальная позиция которой совпадает с текущей позицией T, и т. д.

Хотя теперь, благодаря сказанному в п. 1, 2 § 2, кажется достаточно убедительным, что описанный здесь порядок работы может быть промоделирован на м.Т. с некоторой определенной таблицей, желательно указать конкретный метод сопоставления данной диаграмме некоторой таблицы. Тогда можно было бы использовать диаграммы Тьюринга как вспомогательное средство задания м. Т. Мы опишем такой метод в п. 7.

6. Примеры диаграмм Тьюринга. Дальнейшие упрощения

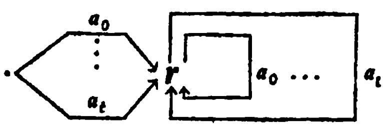
Все машины, входящие в нижеследующие диаграммы, имеют один и тот же рабочий алфавит A_t.

a)



Очевидно, что машина, задаваемая этой диаграммой, работает так же, как и м. Т. из примера а) в п. 2.

b) Машина R



действует следующим образом:

$$\sim \underset{\uparrow}{-}\, w \bigstar \sim \overset{R}{\Longrightarrow} \sim -\, w \underset{\uparrow}{\bigstar} \sim .$$

Оба примера подсказывают дальнейшие упрощения:

(iii) если от некоторого символа к другому для всех $j=0, \ldots, t$ ведет стрелка с буквой a_j, то все эти стрелки могут быть заменены одной-единственной стрелкой *без букв*;

(iv) если среди стрелок, ведущих от одного символа к другому, не хватает лишь нескольких из всех возможных, то все имеющиеся стрелки могут быть заменены одной, на которой должны быть написаны буквы отсутствующих стрелок со знаком неравенства $\neq$ перед ними;

(v) если точка соединена всеми стрелками только с одним символом, то она может быть опущена, но упомянутый символ должен быть выделен как *начальный символ*: обведен кружком или помещен левее всех остальных;

(vi) наконец, можно опускать ненадписанную стрелку, связывающую два символа, стоящие один за другим, и писать M^n вместо $\underbrace{M \ldots M}_{n \text{ раз}}$.

Пример a) после упрощения примет вид

$$r^3 a_0,$$

пример b):

$$\begin{tikzcd} r \arrow[loop above, "\neq a_0"] \end{tikzcd}$$

Дальнейшее упрощение касается рабочих алфавитов машин, входящих в диаграмму. Выше мы потребовали, чтобы все машины имели один и тот же рабочий алфавит, и тогда он же становится рабочим алфавитом машины, определяемой диаграммой. Мы примем здесь еще следующее соглашение: если для диаграммы D выбран алфавит A_t и если T есть символ некоторой м. Т. с меньшим рабочим алфавитом A_s, то этот символ T можно употреблять как обозначение для таких м. Т. из D, таблицы которых совпадают с таблицей T после добавления к ней для каждого состояния и каждой буквы a из $A_t - A_s$ строки $qasq$[1]).

---

[1]) Символы, обозначающие некоторую м. Т. для всякого рабочего алфавита, например r или L, мы будем всегда использовать в диаграммах таким образом, чтобы они обозначали машину с тем же рабочим алфавитом, что и у машины, описываемой заданной диаграммой.

7. Построение таблиц по диаграммам

Разъяснение порядка работы машины, заданной некоторой (неупрощенной) диаграммой, подсказывает следующий способ построения таблицы машины по ее диаграмме. (Мы определим эту таблицу «с точностью до нумерации ее состояний»; в самом деле, для нас прежде всего важен порядок, согласно которому м. Т. переходит от одной позиции к другой после применения ее к произвольной начальной позиции. Однако легко понять, что при этом нумерация состояний, исключая состояние q_0, не играет никакой роли. Кроме того, нижеследующая конструкция может быть уточнена таким образом, чтобы нумерация состояний определялась однозначно.)

Сначала (например, посредством индексации многократно встречающихся в диаграмме символов) мы добьемся того, чтобы каждый символ входил в диаграмму только однажды (это нужно лишь для упрощения описания процесса). Затем мы сопоставим каждому символу соответствующую таблицу, перепишем таблицы одну за другой в любой последовательности и введем новую сплошную нумерацию состояний всех таблиц, начиная с состояния q_1. При этом состояние q_0 таблицы, соответствующей символу M, заменяется новым состоянием q_M.

Теперь мы добавим следующие строки: для всех a, которым соответствует стрелка, ведущая из точки снова к ней же, строку

$$q_0 a a q_0;$$

для всех a, которым соответствует стрелка, ведущая из точки к символу M, строку

$$q_0 a a q_M,$$

и наконец, для всех a, которым не соответствует никакая стрелка, выходящая из точки, строку

$$q_0 a s q_0.$$

В заключение следует изменить полученную таблицу следующим образом: если два символа M и M' соединены стрелкой с буквой a, то всякую строку

$$q a s q'$$

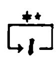
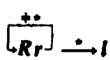
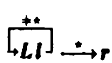
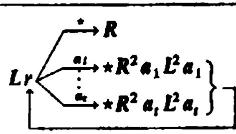
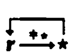
из соответствующей M части таблицы заменяем строкой

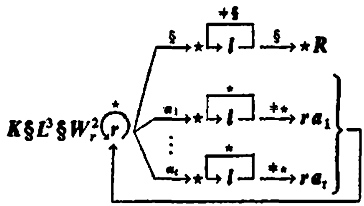
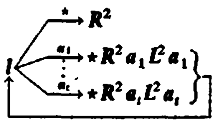
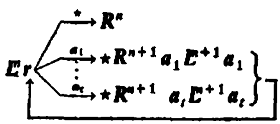
$$qaaq_{M'}.$$

Очевидно, что в результате этих построений мы получим таблицу Тьюринга, причем соответствующая ей машина выполняет те же действия, что и машина, задаваемая диаграммой. Мы можем ввиду этого задавать в дальнейшем м. Т. их диаграммами.

8. Дальнейшие примеры машин Тьюринга

В приведенной ниже таблице даны дальнейшие простые примеры м. Т. Входной алфавит всех машин есть A_t. Некоторые из машин в качестве вспомогательной буквы используют букву a_{t+1}, для которой мы будем пользоваться сокращением §; рабочий алфавит таких машин есть A_{t+1}.

Символ	Действие	Диаграмма
R	$\sim\underset{\uparrow}{\sim}w\star\sim \;\Rightarrow\; \sim\sim w\underset{\uparrow}{\star}\sim$	 (ср. п. 6b)
L	$\sim\star w\underset{\uparrow}{\sim}\sim \;\Rightarrow\; \sim\underset{\uparrow}{\star}w\sim\sim$	
$\mathfrak{R}$	$\sim\underset{\uparrow}{\sim}X\star\star\sim \;\Rightarrow\; \sim\sim X\underset{\uparrow}{\star}\star\sim$	
$\mathfrak{L}$	$\sim\star\star X\underset{\uparrow}{\sim}\sim \;\Rightarrow\; \sim\star\underset{\uparrow}{\star}X\sim\sim$	
K	$\sim\star w\underset{\uparrow}{\star}\ldots$ $\sim\star w\star w\underset{\uparrow}{\star}\ldots$ (копирует)	
W_r	$\sim\underset{\uparrow}{\sim}w\star\sim \;\Rightarrow\; \sim\sim\star\cdots\underset{\uparrow}{\star}\sim$ (стирает справа)	

Символ	Действие	Диаграмма
W_l	$\sim\star w\underset{\uparrow}{\sim}\sim\ \Rightarrow$ $\sim\underset{\uparrow}{\star}\cdots\star\sim\sim$ (стирает слева)	
V	$\sim\star w_1\star w_2\underset{\uparrow}{\star}\ldots\ \Rightarrow$ $\sim\star w_2\underset{\uparrow}{\star}\ldots$ (сдвигает)	
I	$\sim\star w\star\ldots\ \Rightarrow$ $\sim\star w\star w^{-1}\underset{\uparrow}{\star}\ldots$ (строит обратное слово)	
K_n	$\sim\star w_1\star\cdots\star w_n\underset{\uparrow}{\star}\ldots\ \Rightarrow$ $\sim\star w_1\star\cdots\star w_n\star w_1\underset{\uparrow}{\star}\ldots$	

В графе «Действие» используются обозначения, введенные в п. 2, § 2, а также следующие обозначения:

X — для последовательности (быть может, пустой) *непустых* слов $w_1, \ldots, w_n$, разделенных звездочками; так, X при $n=0$ есть пустое слово, при $n>0$ есть $w_1\bigstar\ldots\bigstar w_n$;

w^{-1} — для слова, полученного из w обращением последовательности букв ($[\,]^{-1}=\square$).

Из следующих ниже рассуждений ясно, что рабочая ячейка никогда не попадает на часть ленты, обозначаемую символом $\sim$, так что эта часть ленты никак не влияет на работу машины и, наоборот, машина не изменяет ее содержимого. Далее, очевидно, что отдельные машины действуют правильно и в том случае, когда какие-то слова оказываются пустыми.

Кое-что о работе некоторых из этих м. Т.:

8) K: машина K работает согласно блок-схеме, уже описанной в п. 2 для рабочего алфавита A_t и понятным образом модифицированной для случая A_1.

V: α) Применяя K, мы получаем позицию

$$\sim \bigstar \underset{\cdots\cdots\cdots\cdots}{w_1 \bigstar w_2} \bigstar w_2 \underset{\uparrow}{\bigstar} \ldots,$$

в которой подчеркнутая часть содержит достаточно места, чтобы мы могли перенести туда w_2.

β) Используя $\S L^3 \S$, мы помечаем границы интересующей нас части ленты и получаем

$$\sim \underset{\uparrow}{\S} w_1 \bigstar w_2 \bigstar w_2 \S \bigstar \ldots .$$

γ) Используя W_r^2, мы стираем w_1 и первое w_2 и получаем

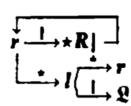
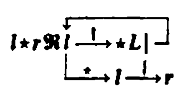
$$\sim \S \bigstar \ldots \underset{\uparrow}{\bigstar} w_2 \S \bigstar \ldots .$$

δ) Теперь мы переносим w_2 буква за буквой на нужное место. (Для того чтобы и в первый раз с помощью $\overset{\bigstar}{\boxed{\to l \to}}$ найти нужное место, мы ввели левый знак §.) То, что работа закончена, устанавливается в тот момент, когда посредством $\overset{\bigstar}{\boxed{\to r \to}}$ мы доходим до правого знака §.

I: машина I работает согласно блок-схеме, аналогичной диаграмме K.

K_n: Машина K_n является обобщением K.

В следующей таблице описаны еще две м. Т. с входным и рабочим алфавитом A_1; они используются в § 4, п. 2.

Символ	Действие	Диаграмма
T_r	$\sim \underset{\uparrow}{\star} X \star \ldots \Rightarrow$ $\sim \star \underset{\uparrow}{\star} X \star \ldots$ (перенос направо)	
T_l	$\sim \| \| \underset{\uparrow}{\star} X \star \ldots \Rightarrow$ $\sim \| \underset{\uparrow}{\star} X \star \ldots$ (перенос налево)	

T_r: α) Пусть X — непустая последовательность. Тогда после действия r в рабочей ячейке стоит знак $|$. С него начинается слово, сдвигаемое посредством $\bigstar R\,|$ на одну ячейку вправо (вспомним, что слово состоит только из знаков $|$). Если это слово не было последним словом последовательности, то после действия r мы опять найдем в рабочей ячейке знак $|$ и сдвинем следующее слово, и т. д. Если же, наоборот, это слово было последним, то после действия r в рабочей ячейке находится знак $\bigstar$. Так как X не пусто, то после действия l в рабочей ячейке стоит знак $|$, и посредством L мы пробежим всю сдвинутую последовательность.

β) Пусть X — пустая последовательность. Тогда одна за другой реализуются позиции

$$\sim\underset{\uparrow}{\bigstar}\bigstar\ldots,\qquad \sim\bigstar\underset{\uparrow}{\bigstar}\ldots,\qquad \sim\underset{\uparrow}{\bigstar}\bigstar\ldots,\qquad \sim\bigstar\underset{\uparrow}{\bigstar}\ldots,$$

так что и в этом случае T_r останавливается в нужной конечной позиции.

T_l: После того как посредством $l\bigstar rR$ получена позиция

$$\sim|\bigstar\bigstar X\underset{\uparrow}{\bigstar}\ldots,$$

T_l работает совершенно аналогично T_r. Непосредственно перед вступлением в действие машины l, из которой выходит стрелка $\xrightarrow{\bigstar}$, в случае непустой последовательности X достигается позиция

$$\sim|\underset{\uparrow}{\bigstar}X\bigstar\ldots,$$

а в случае пустой X — позиция

$$\sim|\bigstar\underset{\uparrow}{\bigstar}\ldots.$$

Теперь остается еще проверить, какой из двух случаев ($\bigstar$ или $|$) имеет место, и остановиться в нужной позиции.

9. Доказательство вычислимости по Тьюрингу некоторых специальных функций

В этом пункте мы определим некоторые специальные функции и построим вычисляющие их м. Т. Знание этих м. Т. и их работы для дальнейшего не обязательно. Поэтому при чтении этого пункта можно опустить те его части, которые посвящены их описанию.

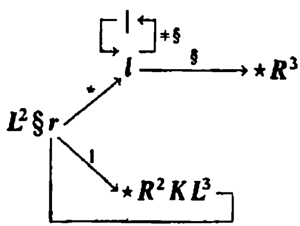
а) *Функция-произведение.* Мы опишем машину P, реализующую *нормированное* вычисление функции-произведения. Итак, после применения к позиции

$$\sim \bigstar w_1 \bigstar w_2 \underset{\uparrow}{\bigstar} \ldots,$$

где w_1 и w_2 — произвольные слова из $\Omega(\{|\})$ (и тем самым, по нашему соглашению, натуральные числа), машина P должна после конечного числа шагов остановиться в позиции

$$\sim \bigstar w_1 \bigstar w_2 \bigstar w_1 \cdot w_2 \underset{\uparrow}{\bigstar} \ldots.$$

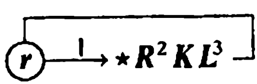
При этом P не должна заходить в ячейки части ленты, обозначаемой $\sim$, и, в частности, не должна изменять записи в этой части. Это осуществляет такая машина:



Замечания по поводу ее работы:

α) При помощи $L^2\S$ мы маркируем ячейку слева от w_1;

β) теперь мы копируем w_2, используя



подряд столько раз, чему равно w_1. Заметим при этом, что K осуществляет переход

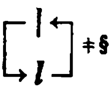
$$\sim \bigstar w_2 \underset{\uparrow}{\bigstar} w_3 \bigstar \ldots \overset{K}{\Longrightarrow} \sim \bigstar w_2 \bigstar w_3 w_3 \underset{\uparrow}{\bigstar} \ldots$$

также и для непустого w_3.

γ) После того как эта машина закончила свою работу мы замечаем, что из заключенного в кружок r веде стрелка к звездочке; в этот момент текущая позици такова:

$$\sim \S \underbrace{\bigstar \ldots \bigstar}_{w'_1 \text{ раз}} \underset{\uparrow}{\bigstar} w_2 \bigstar w_1 \cdot w'_2 \bigstar \ldots .$$

δ) Теперь мы восстанавливаем w_1 с помощью



стираем § и останавливаемся справа от $w_1 \cdot w_2$.

(Следует, в частности, убедиться в том, что машин выполняет нужные действия и в том случае, когда одн или оба множителя равны нулю.)

b) *Взаимно однозначные функции, отображающие* $\Omega(A$ *на* $\Omega(A_s)$. Для каждого t и каждого s мы определи взаимно однозначную функцию $\gamma_{t,s}$ на $\Omega(A_t)$ со знач ниями на $\Omega(A_s)$ и покажем, что она и ее обратная фун ция вычислимы по Тьюрингу. Достаточно, очевидно, ра смотреть случай $s = 1$. Действительно, положив при $s >$

$$\gamma_{t,s}(w) = \gamma_{s,1}^{-1}(\gamma_{t,1}(w)),$$

мы получим

$$\gamma_{t,s}^{-1}(w) = \gamma_{t,1}^{-1}(\gamma_{s,1}(w)).$$

Если функции $\gamma_{t,1}$ определены для всех t так, чт они и их обратные функции вычислимы по Тьюрингу то $\gamma_{t,s}$ и $\gamma_{t,s}^{-1}$ также будут в. Т. функциями, поскольк суперпозиции в. Т. функций, как мы увидим в § 4, п. 6 также являются в. Т. функциями.

Вместо $\gamma_{t,1}$ мы будем в дальнейшем писать кратко γ В качестве γ_1 можно взять тождественное отображ ние. Эту функцию, а также обратную к ней (конечн также тождественную) вычисляет машина.

Пусть далее $t > 1$. Функция, определяемая рекуррентным соотношением

$$\gamma_t(\square) = 0,$$
$$\gamma_t(wa_i) = \gamma_t(w)\cdot t + i \text{ при } 1 \leqslant i \leqslant t,$$

и будет искомой. Вычисление осуществляется машиной

$$\textcircled{L}\; r \begin{array}{l} \xrightarrow{\star} R \\ \left.\begin{array}{l} \xrightarrow{a_1} \star R^2 (r|)^t r P V^2 (|r)^1 L \\ \quad\vdots \qquad\qquad\qquad\qquad\qquad \vdots \\ \xrightarrow{a_t} \star R^2 (r|)^t r P V^2 (|r)^t L \end{array}\right\} \end{array}$$

Чтобы пояснить действие машины, предположим, что в ходе вычислений произошел переход от позиции

$$\bigstar\, w_1 w_2 \underset{\uparrow}{\bigstar} \ldots$$

к позиции

$$\bigstar \ldots \bigstar\, w_2' \underset{\uparrow}{\bigstar}\, \gamma_t(w_1) \bigstar \ldots,$$

и далее должна работать машина L в кружке. (В случае когда $w_1 = \square$, это соответствует также началу вычислений!)

Дальше происходит следующее:

α) Lr приводит нас к первой букве слова w_2, если $w_2 \neq \square$, и к звездочке перед $\gamma_t(w_1)$, если $w_2 = \square$ (в этом случае вычисление окончено и нам остается только применить R, чтобы стать справа от значения функции). Если же мы обнаруживаем собственную букву из A_t, вычисления должны быть продолжены.

β) $\bigstar R^2$ стирает эту букву (например, a_i) и перемещается вправо от $\gamma_t(w_1)$. Используя $(r|)^t$, мы получаем число t, а r перемещает нас еще на одну ячейку вправо. Текущая позиция выглядит теперь так:

$$\bigstar \ldots \bigstar\, 'w_2 \bigstar\, \gamma_t(w_1) \bigstar\, t \underset{\uparrow}{\bigstar} \ldots .$$

Здесь штрих перед w_2 указывает, что первая буква стерта.)

γ) Применяя P, получаем

$$\bigstar \ldots \bigstar'\, w_2 \bigstar\, \gamma_t(w_1) \bigstar\, t \bigstar\, \gamma_t(w_1)\cdot t \underset{\uparrow}{\bigstar} \ldots ,$$

δ) V^2 дает нам

$$\bigstar \ldots \bigstar' w_2 \bigstar \gamma_t(w_1)\cdot t \underset{\uparrow}{\bigstar} \ldots ,$$

ε) а $(|r)^i$ дает

$$\bigstar \ldots \bigstar' w_2 \bigstar \gamma_t(w_1)\cdot t+i \underset{\uparrow}{\bigstar} \ldots ,$$

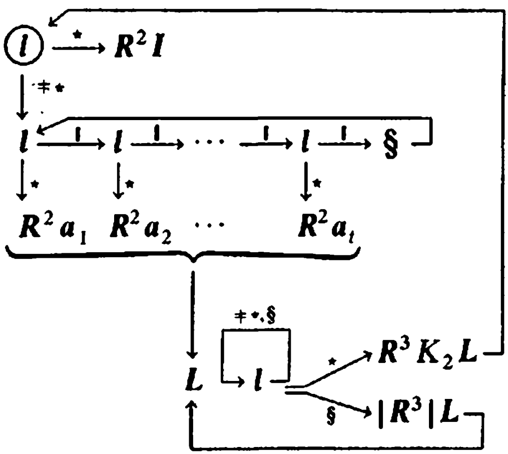
но $\gamma_t(w_1)\cdot t+i$ и есть как раз $\gamma_t(w_1 a_i)$.

ζ) Применяя еще раз L, мы оказываемся между двумя словами и снова получаем нашу начальную позицию, но с сократившимся на одну букву словом w_2:

$$\bigstar \ldots \bigstar' w_2 \underset{\uparrow}{\bigstar} \gamma_t(w_1 a_i) \bigstar \ldots .$$

Вычисление продолжается по тому же плану до тех пор, пока мы не исчерпаем w_2 (см. α).

Функцию γ_t^{-1} вычисляет такая машина:



Чтобы пояснить действие машины, предположим, что в ходе вычислений произошел переход от начальной позиции

$$\bigstar \gamma_t(w_1 w_2) \underset{\uparrow}{\bigstar} \ldots$$

к текущей позиции

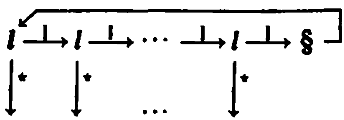
$$\sim \bigstar \gamma_t(w_1) \underset{\uparrow}{\bigstar} w_2^{-1} \bigstar \ldots$$

и что теперь должна работать машина l в кружке (в случае $w_2 = \square$ это также соответствует началу вычислений!).

Далее происходит следующее:

α) Сдвигаясь на одну ячейку влево, мы проверяем, равняется ли $\gamma_t(w_1)$ нулю (т. е. пустому слову). Это имеет место, если мы увидим звездочку. Практически вычисления окончены, так как это означает, что и w_1 есть пустое слово; нам остается только переместиться правее w_2^{-1} и обратить это слово с помощью I.

β) В противном случае нужно найти числа i, $1 \leqslant i \leqslant t$, и $\gamma_t(w_1')$, удовлетворяющие соотношению $\gamma_t(w_1) = \gamma_t(w_1') \cdot t + i$ (w_1' отличается от w_1 отсутствием последней буквы). Если такие числа найдены, то $w_1 = w_1' a_i$. Оба этих действия одновременно выполняются устройством

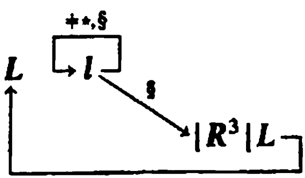


Число знаков §, которые были напечатаны в ходе работы этого фрагмента машины вместо букв слова $\gamma_t(w_1)$, равно $\gamma_t(w_1')$, а значение i устанавливается по тому, после какого по счету из шагов l мы встречаем букву $\bigstar$. После работы машины $R^2 a_i$ мы получаем позицию

$$\sim \bigstar \sim \bigstar\, w_2^{-1} \underset{\uparrow}{a_i} \bigstar \ldots .$$

(Символ $\sim$ обозначает слово $\gamma_t(w_1')$, искаженное печатанием букв §.)

γ) Теперь мы должны еще определить $\gamma_t(w_1')$. Для этого подсчитываем число букв § в $\sim$, используя фрагмент



который действует следующим образом:

L пробегает всю часть $\sim$ записи, а $\overset{\neq\bigstar,\S}{\boxed{\longrightarrow l -}}$ приводит нас к первой букве § в $\sim$ (если такая вообще имеется); далее мы заменяем § на | и с помощью $R^3|$ добавляем справа от уже построенного числа букв § в $\sim$ еще одну букву |. С помощью L мы возвращаемся к правому концу $w_2^{-1}\,a_i$ и можем повторить эту часть процедуры.

δ) Когда же $\overset{\neq\bigstar,\S}{\boxed{\longrightarrow l -}}$ приводит нас к ★, это означает, что все § подсчитаны и мы находимся в позиции

$$\sim \underset{\uparrow}{\bigstar}\, \gamma_t(w_1) \bigstar w_2^{-1}a_i \bigstar \gamma_t(w_1') \bigstar \ldots .$$

ε) Используя R^3K_2L, мы получаем позицию

$$\sim \bigstar \gamma_t(w_1) \bigstar w_2^{-1}\,a_i \bigstar \gamma_t(w_1') \underset{\uparrow}{\bigstar}\, w_2^{-1}a_i \bigstar \ldots,$$

т. е. снова нашу исходную позицию (два первых слова нас больше не интересуют), только с укороченным на одну букву w_1. Вычисления повторяются по той же схеме до полного исчерпания w_1 (когда $\gamma_t(w_1) = \square$, см. α).

c) *n-членные функции*. Мы определим для каждых t и n взаимно однозначную функцию σ_n^t, отображающую $\Omega^n(A_t)$ на $\Omega(A_t)$, так чтобы и она сама, и ее «обратные функции» были вычислимы по Тьюрингу. «Обратными функциями» к σ_n^t следует называть одноместные функции $\sigma_{n,i}^t\,(1 \leqslant i \leqslant n)$ на $\Omega(A_t)$, для которых

$$\sigma_n^t(\sigma_{n,1}^t(w), \ldots, \sigma_{n,n}^t(w)) = w,$$
$$\sigma_{n,i}^t(\sigma_n^t(w_1, \ldots, w_n)) = w_i \text{ при } 1 \leqslant i \leqslant n.$$

Достаточно рассмотреть случай, когда $t = 1$. Действительно, полагая при $t > 1$

$$\sigma_n^t(w_1, \ldots, w_n) = \gamma_t^{-1}(\sigma_n^1(\gamma_t(w_1), \ldots, \gamma_t(w_n))),$$

мы получаем

$$\sigma_{n,i}^t(w) = \gamma_t^{-1}(\sigma_{n,i}^1(\gamma_t(w)))$$

и тем самым достигаем желаемого (так же, как и в примере b)).

Вместо σ_n^1 и $\sigma_{n,i}^1$ мы будем кратко писать σ_n и $\sigma_{n,i}$.

Далее достаточно рассмотреть случай $n=2$. Действительно, положив при $n>2$

$$\sigma_n(w_1, \ldots, w_n)=\sigma_2(\sigma_{n-1}(w_1, \ldots, w_{n-1}), w_n),$$

получим

$$\sigma_{n,i}(w)=\sigma_{n-1,i}(\sigma_{2,1}(w)) \text{ при } 1\leqslant i\leqslant n-1,$$
$$\sigma_{n,n}(w)=\sigma_{2,2}(w)$$

и тем самым, как и выше, достигнем цели (проводя индукцию по n).

Прежде чем построить одну из возможных функций σ_2, проведем следующее вспомогательное рассуждение.

Из каждого слова $w\in\Omega(A_2)$, содержащего хотя бы одну букву a_2, можно однозначно выделить слова w_1 и w_2 так, чтобы

$$w=w_1a_2w_2,\quad w_1\in\Omega(A_1).$$

Поэтому отображение

$$(w_1, w_2)\longmapsto w_1a_2w_2$$

множества $\Omega(A_1)\times\Omega(A_2)$ на множество слов из $\Omega(A_2)$, содержащих хотя бы одну букву a_2, является взаимно однозначным. Подмножество слов $\Omega(A_2)$, не содержащихся в образе этого отображения, совпадает с $\Omega(A_1)$.

Отображение σ множества $\Omega^2(A_1)$ в $\Omega(A_2)$, задаваемое формулами

$$\sigma(w_1, w_2)=\begin{cases} w_2, & \text{если } w_1=0,\\ (w_1-1)\,a_2\gamma_2^{-1}(w_2), & \text{если } w_1\neq 0,\end{cases}$$

является взаимно однозначным отображением $\Omega^2(A_1)$ на $\Omega(A_2)$.

Мы определим теперь

$$\sigma_2(w_1, w_2)=\gamma_2(\sigma(w_1, w_2)).$$

Таким образом, σ_2 есть взаимно однозначная функция на $\Omega^2(A_1)$ со значениями на $\Omega(A_2)$.

α) Вычисление σ_2 осуществляет машина Тьюринга

$$L^2 r \begin{array}{l} \overset{*}{\nearrow} RM_2 \\ \underset{|}{\searrow} R^2M_1K_3K_2La_2^-RM_2 \end{array}$$

При этом M_1 есть символ м. Т., нормированно вычисляющей γ_2^{-1}, а M_2 есть символ м. Т. для нормированного вычисления γ_2. В b) мы построили м. Т. для (ненормированного) вычисления γ_2 и γ_2^{-1}. Но, как будет видно из п. 3 § 4, существуют м. Т. и для нормированного вычисления этих функций.

β) $\sigma_{2,1}$ вычисляет машина

$$\begin{tikzcd} M_1 L \arrow[r] & r \arrow[loop above, "\neq *, a_2"] \arrow[r, "a_2"] \arrow[dr, "*"'] & \star R K_2 \mid r. \\ & & r \end{tikzcd}$$

γ) $\sigma_{2,2}$ вычисляет машина

$$\begin{tikzcd} M_1 L \arrow[r] & r \arrow[loop above, "\neq *, a_2"] \arrow[r, "a_2"] & \star R M_2 . \end{tikzcd}$$

Выяснение подробностей работы этих трех машин мы оставляем читателю.

10. Представление машины Тьюринга посредством диаграммы, составленной из элементарных машин

Ранее мы уже употребляли не очень определенное выражение «машина моделирует некоторую другую машину». Для случая, когда обе машины являются м. Т., мы можем ввести следующее уточнение.

Мы скажем, что м. Т. M моделирует м. Т. M' (в сильном смысле; в п. 2 § 4 мы познакомимся с несколько более слабым понятием моделирования), если выполнены такие условия:

(i) Данная начальная позиция вызывает машинный останов (соотв. переход за край ленты) M после конечного числа шагов тогда и только тогда, когда та же начальная позиция вызывает машинный останов (соотв. переход за край ленты) M' также после конечного числа шагов. В обоих случаях конечные позиции M и M' должны совпадать.

(ii) Последовательность текущих позиций машины M для данной начальной позиции является подпоследовательностью последовательности текущих позиций машины M' для той же начальной позиции.

Справедлива следующая теорема:

Теорема. *Каждой таблице Тьюринга T над алфавитом $\mathbf{A}_t$ можно эффективным образом сопоставить диаграмму D, образованную символами $\mathbf{r}$, $\mathbf{l}$, $\mathbf{a}_0, \ldots, \mathbf{a}_t$ и точкой, так, чтобы определяемая этой диаграммой м. Т. моделировала м. Т. с таблицей T.*

Доказательство. Такая диаграмма может быть получена следующим образом.

Каждой строке $qavq'$ из T, в которой v не совпадает с $\mathbf{s}$, мы сопоставим на диаграмме символ v. В связи с этим мы назовем его символом, *соответствующим* строке $qavq'$. Кроме того, мы поместим в диаграмму символ $\cdot$ (точку).

Теперь мы соединим для всех $j = 0, \ldots, t$

a) точку — с символом, соответствующим строке $q_0\mathbf{a}_j\ldots$;

b) каждый символ, соответствующий строке $\ldots q$, — с символом, соответствующим строке $q\mathbf{a}_j\ldots$,

стрелкой с буквой $\mathbf{a}_j$, если только упомянутый символ вообще должен быть написан, т. е. если соответствующее действие отлично от $\mathbf{s}$.

Очевидно, что это и будет искомая диаграмма. Доказательство свойств (i) и (ii) мы оставляем читателю.

§ 4. *Нормированная вычислимость по Тьюрингу*

В этом параграфе будет доказано, что всякая в. Т. функция является нормированно в. Т. функцией, причем соответствующая м. Т. не использует никаких вспомогательных букв. (По поводу определения нормированно в. Т. функций см. § 2.) Для этого мы построим в несколько этапов из м. Т. T, вычисляющей f, некоторую м. Т., не использующую вспомогательных букв и нормированно вычисляющую f. Промежуточные этапы построения описаны в п. 1—3; в п. 4, 5 строятся две используемые нами вспомогательные машины, а в п. 6 доказывается одно простое следствие основной теоремы этого параграфа.

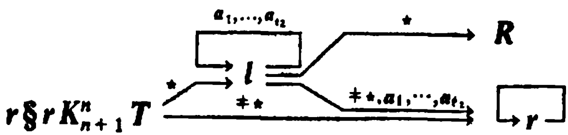
1. Машина $T^{\S}$

Пусть f есть некоторая n-местная функция с входным алфавитом $E = A_{t_1}$ и выходным алфавитом $B = A_{t_2}$:

$$f: \Omega^n (A_{t_1}) \longrightarrow \Omega (A_{t_2}).$$

Машина T вычисляет f, используя рабочий алфавит $A_t \supset E \cup B$. Знак § служит, как обычно, сокращением для a_{t+1}.

Рассмотрим следующую машину с рабочим алфавитом A_{t+1}, которую мы обозначим через $T^{\S}$:



(Напомним о нашем соглашении добавлять в этом случае к каждому состоянию q таблицы T строку $q \S s q$.)

После применения к позиции

$$\underset{\uparrow}{\bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar} \ldots$$

эта м. Т. производит следующие действия:

α) После работы $r \S r K^n_{n+1}$ возникает позиция

$$\bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar \S \bigstar w_1 \bigstar \ldots \bigstar w_n \underset{\uparrow}{\bigstar} \ldots .$$

β) Теперь работает машина T. Она либо никогда не останавливается (в этом случае, очевидно, $f(w_1, \ldots, w_n)$ не определена), либо имеет место машинный останов. Перехода за край ленты не бывает, так как машина не может переместиться левее знака §. При этом могут возникнуть разные ситуации:

γ_1) T останавливается на собственной букве. Если это §, то из начальной позиции

$$\bigstar w_1 \bigstar \ldots \bigstar w_n \underset{\uparrow}{\bigstar} \ldots$$

T после конечного числа шагов переходит за край ленты, во всех остальных случаях T также останавливается на этой букве. В обоих случаях $f(w_1, \ldots, w_n)$ не определена. В $T^{\S}$ после этого работает машина $\boxed{\to r}$. Таким образом, в этом случае $T^{\S}$ никогда не останавливается.

γ_2) T останавливается на пустой букве. Это означает, что мы остановились после некоторого слова w. Исходная машина T, примененная к позиции

$$\bigstar w_1 \bigstar \ldots \bigstar w_n \underset{\uparrow}{\bigstar} \ldots,$$

останавливается после того же слова, если оно не начинается с буквы §. В случае когда $w = \S w'$, T останавливалась в позиции

$$] w' \underset{\uparrow}{\bigstar} \sim .$$

Это означает, что $f(w_1, \ldots, w_n)$ определена (и принимает значение w) в том и только том случае, когда w содержит только буквы из B.

Так это или нет, выясняет машина

$$\begin{tikzcd} l \arrow[loop above, "a_1,\ldots,a_{t_2}"] \end{tikzcd}$$

Если она приходит к $\bigstar$, то мы действительно находились после значения функции. В $T^{\S}$ следующей работает машина R, и мы вновь оказываемся непосредственно после значения функции.

Если же мы приходим не к $\bigstar$, то $f(w_1, \ldots, w_n)$ не определена. В этом случае следующей в $T^{\S}$ работает машина $\begin{tikzcd} r \arrow[loop above] \end{tikzcd}$ и, таким образом, $T^{\S}$ никогда не останавливается.

Объединяя эти выводы, мы получаем следующее описание работы $T^{\S}$. После применения к позиции

$$\bigstar w_1 \bigstar \ldots \bigstar w_n \underset{\uparrow}{\bigstar} \ldots$$

a) T никогда не останавливается, если $f(w_1, \ldots, w_n)$ не определена;

b) T останавливается после $f(w_1, \ldots, w_n)$ в противном случае.

2. Моделирование над алфавитом $\{|\}$

Рассмотрим м. Т. M с рабочим алфавитом A_m. Произвольной записи на ленте M можно сопоставить несобственное слово над A_m, выписав подряд все буквы записи слева направо вплоть до любой ячейки, правее которой нет собственных букв записи. Разные слова, которые могут быть сопоставлены такой записи, отличаются друг от друга только различным числом букв ★ на правом краю. Каждому несобственному слову соответствует единственная запись, так что оно может быть использовано для представления этой записи. Например, слова

$$a_0a_3a_6a_0a_0 \text{ и } a_0a_3a_6$$

представляют одну и ту же запись

$$] \bigstar\, a_3a_6 \bigstar \ldots .$$

При изучении какой-нибудь определенной позиции мы будем допускать в качестве представления ее записи только такие слова, в которых указывается содержимое рабочей ячейки (даже если она пуста вместе со всеми ячейками, лежащими справа от нее).

Произвольное несобственное слово w над A_m может быть закодировано несобственным словом над A_1. Для этого вместо каждой буквы w пишут последовательность букв |, длина которой на единицу больше индекса соответствующей буквы. Полученные таким образом последовательности отделяют одну от другой знаками ★. Кроме того, знак ★ пишут слева от полученного несобственного слова. Звездочку, предшествующую некоторой последовательности штрихов, соответствующей определенной букве слова w, мы будем называть принадлежащей этой букве. Например, последовательности

★||||★|||||||★|★| и ★|★||||★||||||| .

кодируют соответственно слова

$$a_0a_3a_6a_0a_0 \quad \text{и} \quad a_0a_3a_6.$$

Предположим теперь, что задана некоторая позиция S с записью из букв A_m и что некоторое допустимое слово w, несобственное над A_m, представляет эту запись. Закодируем w несобственным словом над A_1 и напишем это слово на ленте Тьюринга. Место рабочей ячейки мы укажем согласно следующему правилу. В рабочей ячейке позиции S находится некоторая буква, в любом случае входящая также и в w, так как w является допустимым словом. В закодированном слове w этой букве соответствует некоторый знак ★. Мы примем за рабочую ту ячейку, в которой находится этот знак ★. Тем самым мы сопоставим позициям с записями над A_m позиции с записями над A_1. Например, позиции $)\bigstar\, a_3 a_6 \bigstar \underset{\uparrow}{\bigstar} \ldots$ соответствует позиция

$$)\bigstar|\bigstar||||\bigstar|||||||\bigstar|\underset{\uparrow}{\bigstar}|\bigstar|\bigstar\ldots.$$

Каждую позицию, сопоставленную S, мы будем обозначать символом $\bar{S}$. По каждой $\bar{S}$ можно очевидным образом построить S. Позиция $\bar{S}$ определена однозначно с точностью до количества комбинаций ★|, следующих за последней собственной буквой ее записи.

Теперь мы построим из M машину $\bar{M}$ со следующими свойствами:

(i) Из начальной позиции S машина M после конечного числа шагов приходит к машинному останову (соотв. переходит за край ленты) тогда и только тогда, когда машина $\bar{M}$ из начальной позиции $\bar{S}$ (с любым кодировочным словом $\bar{S}$, соответствующим S) после конечного числа шагов также приходит к машинному останову (соотв. переходит за край ленты). В обоих случаях конечная позиция $\bar{M}$ есть некоторая позиция $\bar{S}_E$, где S_E — конечная позиция M.

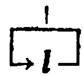
(ii) Пусть из начальной позиции S_0 машина M пробегает (возможно, бесконечную) последовательность позиций S_0, S_1, ... Тогда любая последовательность позиций, пробегаемая $\bar{M}$ из начальной позиции $\bar{S}_0$, содержит в качестве подпоследовательности $\bar{S}_0$, $\bar{S}_1$, ...

(Ср. эти требования с нашими требованиями (i), (ii) из § 3, п. 10. Мы назовем такое поведение $\bar{M}$ по отношению к M моделированием.)

Мы построим такую $\bar{M}$ следующим образом:

(1) При помощи одних только символов элементарных машин $\boldsymbol{r}$, $\boldsymbol{l}$, $\boldsymbol{a}_0$, ..., $\boldsymbol{a}_m$ и точки построим диаграмму, моделирующую машину $\bar{M}$ (ср. п. 10 § 3). Затем, следуя правилам (2)—(4), заменим все символы, кроме точки,

(2) Каждый символ l мы заменяем символом машины



Эта машина за конечное число шагов переводит позицию

$$\sim\bigstar\underbrace{|\ldots|}_{i+1}\underset{\uparrow}{\bigstar}\underbrace{|\ldots|}_{j+1}\bigstar\sim, \qquad \text{т. е.}\quad \overline{\sim a_i\underset{\uparrow}{a_j}\sim},$$

в конечную позицию

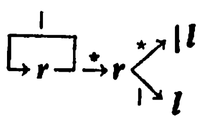
$$\sim\underset{\uparrow}{\bigstar}\underbrace{|\ldots|}_{i+1}\bigstar\underbrace{|\ldots|}_{j+1}\bigstar\sim, \qquad \text{т. е.}\quad \overline{\sim\underset{\uparrow}{a_i}a_j\sim},$$

с машинным остановом, а из начальной позиции

$$]\underset{\uparrow}{\bigstar}\underbrace{|\ldots|}_{i+1}\bigstar\sim, \qquad \text{т. е.}\quad \overline{]\underset{\uparrow}{a_i}\sim},$$

она переходит за край ленты и не меняет позиции.

(3) Каждый символ r мы заменяем символом м. Т.



Эта м. Т. из позиции

$$\sim\underset{\uparrow}{\bigstar}\underbrace{|\ldots|}_{i+1}\bigstar\underbrace{|\ldots|}_{j+1}\bigstar\sim, \qquad \text{т. е.}\quad \overline{\sim\underset{\uparrow}{a_i}a_j\sim},$$

приходит к машинному останову в позиции

$$\sim\bigstar\underbrace{|\ldots|}_{i+1}\underset{\uparrow}{\bigstar}\underbrace{|\ldots|}_{j+1}\bigstar\sim, \qquad \text{т. е.}\quad \overline{\sim a_i\underset{\uparrow}{a_j}\sim},$$

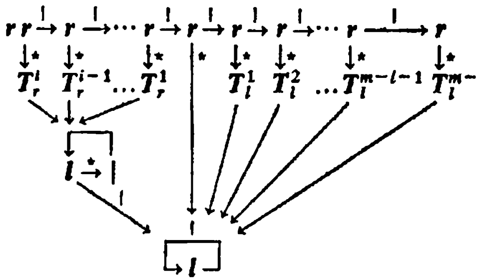
а из позиции

$$\sim\underset{\uparrow}{\bigstar}\underbrace{|\ldots|}_{i+1}\bigstar\ldots, \qquad \text{т. е.}\quad \overline{\sim\underset{\uparrow}{a_i}\bigstar\ldots},$$

приходит к машинному останову в позиции

$$\sim \bigstar \underbrace{|\ldots|}_{i+1} \underset{\uparrow}{\bigstar} | \bigstar \ldots, \qquad \text{т. е.}\ \overline{\sim a_i \underset{\uparrow}{\bigstar} \ldots}\ .$$

(4) Каждый символ a_i мы заменяем символом м. Т.



Эта м. Т. после применения к начальной позиции

$$\underset{\uparrow}{\sim} \bigstar \underbrace{|\ldots|}_{j+1} \bigstar \sim \ldots, \qquad \text{т. е.}\ \overline{\underset{\uparrow}{\sim} a_j \sim},$$

выполняет $(j+2)$ раза операцию r и попадает в ячейку со знаком $\bigstar$. Затем работает фрагмент машины, на который указывает стрелка $\xrightarrow{\bigstar}$, выходящая из последнего выполненного r.

а) $j < i$. Этот машинный фрагмент есть T_r^{i-j}. В результате его работы вся (содержательная) часть записи, стоящая справа от текущей рабочей ячейки, сдвигается вправо на $i-j$ ячеек. (Отметим, что если $\overline{M}$ удовлетворяет нашим требованиям, то мы получим в этот момент позицию, в которой справа от рабочей ячейки находится некоторая конечная последовательность символов, правее которой имеются только пустые ячейки.) Мы получили позицию

$$\sim \bigstar \underbrace{|\ldots|}_{j+1} \underbrace{\bigstar \ldots \bigstar}_{i-j} \underset{\uparrow}{\bigstar} \sim.$$

Применяя $\boxed{l \xrightarrow{\bigstar} |}$, мы заменяем $i-j$ звездочек штрихами; в заключение мы смещаемся влево от полученной последовательности $i+1$ штрихов. Конечная позиция в этом случае, как и требовалось, имеет вид

$$\overline{\sim \underset{\uparrow}{a_i} \sim}.$$

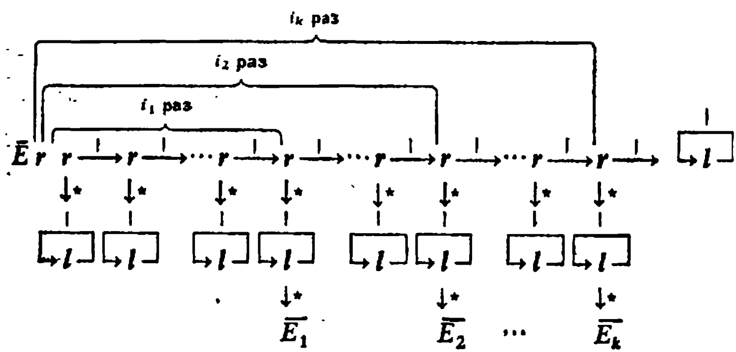
b) $j=i$. Мы установили, что «в рабочей ячейке стоит a_i»[1]), и должны теперь «напечатать в рабочей ячейке букву a_i». Нам остается только вернуться к знаку ★, принадлежащему a_i.

c) $j>i$ (но $j \leqslant m$). Мы установим, что «в рабочей ячейке стоит буква a_j с большим, чем i, индексом». Путем $(j-i)$-кратного применения операции T_l мы добьемся того, что «индекс буквы уменьшится до i», и одновременно сдвинем влево последовательность, стоящую справа от «a_j». В заключение мы вернемся к знаку ★, принадлежащему a_i.

Любой символ новой диаграммы, соответствующий, согласно (2), (3), (4), определенному символу E элементарной машины в старой диаграмме, мы будем обозначать буквой $\bar{E}$.

(5) Теперь мы устраним все старые стрелки и введем новые стрелки и дополнительные символы.

Пусть в старой диаграмме символ E был связан стрелками $\xrightarrow{a_{i_1}}, \ldots, \xrightarrow{a_{i_k}}$ с символами $E_1, \ldots, E_k$, и пусть никаких других стрелок, начинающихся в E, нет. Тогда мы соединим $\bar{E}$ с $\bar{E}_1, \ldots, \bar{E}_k$ следующим образом:



1) Мы пользуемся кавычками, чтобы выразить в краткой форме высказывания относительно $\bar{S}$ посредством высказываний относительно S.

Таким образом, сначала мы выясняем тем же способом, что и в (4), «какая буква находится в рабочей ячейке», возвращаемся к знаку ★, принадлежащему этой букве, переходим к $\bar{E}_1$, если «эта буква есть a_{i_1}», и т. д. Если «ни одна из букв $a_{i_1}, \ldots, a_{i_k}$ не находится в рабочей ячейке», то $\bar{M}$ после возвращения останавливается, так как в этом случае останавливалась и M.

Из объяснений (2)—(5) очевидно, что построенная по указаниям (1)—(5) м.Т. требуемым образом моделирует машину M. Рабочий алфавит $\bar{M}$ может быть выбран произвольным, нужно только, чтобы он содержал знак |. Но наше соглашение об алфавитах гарантирует это для любого алфавита.

3. Нормированное вычисление по Тьюрингу

Применив описанную в п. 2 конструкцию к нашей м.Т T^f, построенной в п. 1, мы получим м.Т. $\bar{T}^f$ со следующими свойствами (в качестве рабочего алфавита мы возьмем алфавит $A_{\max\{t_1, t_2\}}$ (ср. п. 1)).

После применения к позиции

$$S := \overline{\bigstar\, w_1 \bigstar \ldots \bigstar\, w_n \underset{\uparrow}{\bigstar}} \ldots,$$

где $w_1, \ldots, w_n$ — произвольные слова из $\Omega(A_{t_1})$, она останавливается через конечное число шагов тогда и только тогда, когда определено значение функции $f(w_1, \ldots, w_n)$. В этом случае происходит машинный останов в конечной позиции

$$\bigstar X_1 \overline{\bigstar\, f(w_1, \ldots, w_n) \underset{\uparrow}{\bigstar}} \bigstar X_2 \bigstar \ldots.$$

При этом X_1 и X_2 — произвольные (может быть, пустые) ряды последовательностей штрихов, в остальном нас не интересующие (если X_1 — пустой ряд, то соответствующий ему знак ★ должен также отсутствовать).

Так как машина $\bar{T}^f$ в ходе вычислений с начальной позицией S никогда не получает указания о сдвиге влево, если она оказалась в ячейке с номером 0 (иначе произойдет уход за пределы ленты), то можно произвольным образом сдвинуть запись позиции S вправо и записать в освободившуюся часть ленты произвольный набор букв

$$\sim\overline{\bigstar w_1\bigstar\ldots\bigstar w_n}\underset{\uparrow}{\bigstar}\ldots;$$

часть записи $\sim$ не повлияет на ход вычислений и при этом сама не изменится; конечная позиция будет следующей:

$$\sim\bigstar X_1\overline{\bigstar f(w_1,\ldots,w_n)}\underset{\uparrow}{\bigstar}\bigstar X_2\bigstar\ldots.$$

В качестве $\sim$ мы возьмем $\bigstar w_1\bigstar\ldots\bigstar w_n\bigstar$. Для этого случая мы получим: машина $\overline{T}^{s}$ после применения к позиции

$$\bigstar w_1\bigstar\ldots\bigstar w_n\bigstar\overline{\bigstar w_1\bigstar\ldots\bigstar w_n}\underset{\uparrow}{\bigstar}\ldots$$

останавливается через конечное число шагов тогда и только тогда, когда значение $f(w_1,\ldots,w_n)$ определено. В этом случае конечной позицией будет позиция

$$\bigstar w_1\bigstar\ldots\bigstar w_n\bigstar\bigstar X_1\overline{\bigstar f(w_1,\ldots,w_n)}\underset{\uparrow}{\bigstar}\bigstar X_2\bigstar\ldots.$$

Если теперь мы построим еще машины V_n (*кодирующую машину для n-членных последовательностей*) и E (*декодирующую машину*) с рабочим алфавитом $A_{\max}\{t_1, t_2\}$, которые выполняют действия

$$\bigstar w_1\bigstar\ldots\bigstar w_n\underset{\uparrow}{\bigstar}\ldots\overset{V_n}{\Longrightarrow}$$

$$\overset{V_n}{\Longrightarrow}\bigstar w_1\bigstar\ldots\bigstar w_n\bigstar\overline{\bigstar w_1\bigstar\ldots\bigstar w_n}\underset{\uparrow}{\bigstar}\ldots,$$

соответственно

$$\bigstar w_1\bigstar\ldots\bigstar w_n\bigstar\bigstar X_1\overline{\bigstar w}\underset{\uparrow}{\bigstar}\bigstar X_2\bigstar\ldots\overset{E}{\Longrightarrow}$$

$$\overset{E}{\Longrightarrow}\bigstar w_1\bigstar\ldots\bigstar w_n\bigstar w\underset{\uparrow}{\bigstar}\ldots,$$

то машина $V\overline{T}^{s}E$ будет выполнять требуемое нормированное вычисление по Тьюрингу без вспомогательных букв. Машина V_n строится в п. 4, E—в п. 5.

4. Кодирующая машина для n-членных последовательностей

Мы построим V_n из м.Т. V_{ni}, действующих следующим образом (как обычно, X обозначает ряд последовательностей штрихов):

$$\star w_1 \star \dots \star w_n \star \star X \underset{\uparrow}{\star} \dots \xRightarrow{V_{ni}}$$

$$\xRightarrow{V_{ni}} \star w_1 \star \dots \star w_n \star\star X \overline{w_i \star} \underset{\uparrow}{\star} \dots .$$

Очевидно, что в качестве V_n можно взять машину

$$r^2 | r V_{n1} \dots V_{nn} l^2$$

(подчеркнем, что $\overline{w_i \star}$ имеет вид $\star Y$, где Y есть непустая последовательность).

И наконец, машина V_{ni} может быть реализована следующей м.Т. (при проверке порядка работы следует обратить внимание на то, что некоторые из w_j могут быть пустыми):

$$\mathfrak{L} L^{n-i+2}\, r \begin{cases} \xrightarrow{\star} R^{n-i+1} \mathfrak{R} r (|r)^1 \\ \xrightarrow{a_1} \star R^{n-i+2} \mathfrak{R} r (|r)^2 \mathfrak{L} L^{n-i+2} a_1 \\ \quad\vdots \\ \xrightarrow{a_{t_1}} \star R^{n-i+2} \mathfrak{R} r (|r)^{t_1+1} \mathfrak{L} L^{n-i+2} a_{t_1} \end{cases}$$

Рабочий алфавит машины есть $A_{\max\{t_1, t_2\}}$. Блок-схема V_{ni} аналогична блок-схеме копирующей машины; детали мы оставляем читателю.

5. Декодирующая машина

Для описания несколько более сложной работы декодирующей машины мы займемся сначала ее блок-схемой. При этом для отдельных фрагментов машины мы просто укажем требуемые конечные позиции. Интересующая нас начальная позиция м.Т. E должна быть следующей (ее написание несколько отличается от данного в п. 3):

$$\star w_1 \star \dots \star w_n \star\star X_1 \star | \bar{w} \underset{\uparrow}{\star} | \star X_2 \star \dots .$$

Работа машины может теперь протекать, например, следующим образом:

a) $\sim \bigstar \bigstar X_1 \bigstar | \bar{w} \bigstar | \underset{\uparrow}{\bigstar} X_2 \bigstar \bigstar \ldots$

b) $\sim \bigstar \bigstar X_1 \bigstar | \bar{w} \bigstar | \bigstar \ldots \underset{\uparrow}{\bigstar} \ldots$

c) $\sim \bigstar \bigstar X_1 \bigstar | \bar{w} \underset{\uparrow}{\bigstar} | \bigstar \ldots$

d) $\sim \bigstar \bigstar X_1 \bigstar | \underset{\uparrow}{\bar{w}} \bigstar | \bigstar \ldots$

e) $\sim \underset{\uparrow}{\bigstar} \bigstar \ldots \bigstar \bar{w} \bigstar | \bigstar \ldots$

f) $\sim \bigstar \underset{\uparrow}{|} \bigstar \ldots \bigstar \bar{w} \bigstar | \bigstar \ldots$

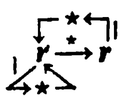
g) $\sim \bigstar | w \underset{\uparrow}{\bigstar} \ldots$

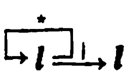
h) $\sim \bigstar w \underset{\uparrow}{\bigstar} \ldots$

При этом положение стрелки в d) должно означать, что рабочая ячейка совпадает с рабочей ячейкой в c), если $w = \square$, в противном случае она совпадает с ячейкой, в которой находится знак $\bigstar$, принадлежащий первой букве слова w.

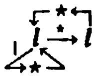
Отдельные процедуры этого ряда выполняют следующие м.Т.:

a) r^2

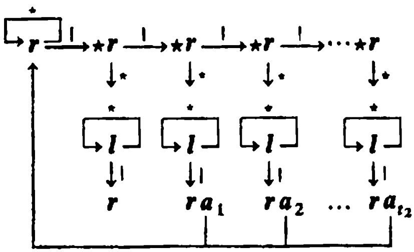
b) 

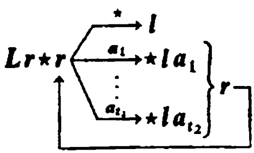
c) 

d) $\overline{Lr}$, т.е. м.Т., получающаяся из Lr с помощью конструкции из п. 2. При этом L и r следует считать м.Т. над A_{l_2}.

e) 

f) $r|$



h) 

Выяснение подробностей работы этих м.Т. мы оставляем читателю.

6. Суперпозиция функций, вычислимых по Тьюрингу

В качестве простого следствия утверждения о том, что всякая в.Т. функция является нормированно в. Т. функцией, мы докажем еще в этом пункте, что суперпозиция в.Т. функций снова будет в.Т. функцией. Точнее, имеет место

Следствие. *Пусть* $g_1, \ldots, g_m$ *суть* n-*местные в.Т. функции на* $\Omega(A_{t_1})$ *со значениями в* $\Omega(A_{t_2})$, *и пусть* h *есть* m-*местная в.Т. функция на* $\Omega(A_{t_2})$ *со значениями в* $\Omega(A_{t_3})$. *Тогда* n-*местная функция* f *на* $\Omega(A_{t_1})$ *со значениями в* $\Omega(A_{t_3})$, *определяемая равенством* [1])

$$f(w_1, \ldots, w_n) = h(g_1(w_1, \ldots, w_n), \ldots, g_m(w_1, \ldots, w_n)),$$

является в.Т. функцией.

---

[1]) Это равенство нужно понимать в том смысле, что если одна (левая или правая) из его частей определена, то определена и другая и при этом выполняется равенство. Чтобы более точно выразить такое положение вещей, иногда используют знак $\simeq$ вместо $=$.

Доказательство. Так как $g_1, \ldots, g_m, h$ являются в.Т. функциями, то существуют м.Т. $T_1, \ldots, T_m, T$, реализующие *нормированное* вычисление этих функций. Теперь мы можем определить следующую м.Т., которая, очевидно, и будет вычислять функцию f:

$$T_1 K^n_{n+1} T_2 K^n_{n+1} T_3 \ldots K^n_{n+1} T_m K_{(m-1)\,n+m} K_{(m-2)\,n+m} \ldots \\ \ldots K_{(m-m)\,n+m} T.$$

Основные позиции в ходе вычислений имеют вид (здесь g_i служит сокращением для $g_i(w_1, \ldots, w_n)$, а f — для $f(w_1, \ldots, w_m)$)

$$\underset{}{\bigstar w_1 \bigstar \ldots \bigstar w_n \underset{\uparrow}{\bigstar} \ldots}$$

$$\bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_1 \underset{\uparrow}{\bigstar} \ldots$$

$$\bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_1 \bigstar w_1 \bigstar \ldots \bigstar w_n \underset{\uparrow}{\bigstar} \ldots$$

$$\bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_1 \bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_2 \underset{\uparrow}{\bigstar} \ldots$$

$$\bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_1 \bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_2 \bigstar \ldots \\ \ldots \bigstar g_{m-1} \bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_m \underset{\uparrow}{\bigstar} \ldots$$

$$\bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_1 \bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_2 \bigstar \ldots \\ \ldots \bigstar g_{m-1} \bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_m \bigstar g_1 \bigstar \ldots \bigstar g_m \underset{\uparrow}{\bigstar} \ldots$$

$$\bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_1 \bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_2 \bigstar \ldots \\ \ldots \bigstar g_{m-1} \bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar g_m \bigstar g_1 \bigstar \ldots \bigstar g_m \bigstar f \underset{\uparrow}{\bigstar} \ldots$$

Детали мы оставляем читателю.

§ 5. Простые примеры неразрешимых множеств

Мы уже выяснили во введении (к части I), что для доказательства неразрешимости некоторого определенного множества необходимо предварительное уточнение понятия алгоритма. В самом деле, такое доказательство является некоторым высказыванием о классе всех возможных алгоритмов. Но при этом этот класс должен быть точно охарактеризован.

Пусть M — множество слов над алфавитом A_t. Согласно нашему определению, M разрешимо тогда и только тогда, когда его характеристическая функция вычислима по Тьюрингу. Однако и здесь еще необходимо уточнение, так как при этом класс допустимых алгоритмов еще «слишком велик».

Нам поможет здесь установленная в § 4 теорема о том, что всякая в.Т. функция может вычисляться на соответствующей м.Т. *без вспомогательных букв.* Отсюда немедленно вытекает

Следствие. *Пусть $M \subset \Omega(A_t)$. Множество M разрешимо тогда и только тогда, когда существует некоторая м.Т. с рабочим алфавитом A_t, вычисляющая характеристическую функцию M.*

Используя это следствие, мы покажем в п. 2 и 3, что некоторые свойства м.Т. неразрешимы. В п. 1 будет предложен способ описания м.Т. словами над их рабочим алфавитом.

1. Машинные слова

До сих пор мы неизменно стояли на той точке зрения, что всякая м.Т. описывается своей таблицей. Таблицы задавались таким образом, что строки писались одна под другой; однако строки могут, конечно, писаться и одна за другой в один ряд. Если при этом символы состояний, а также символы r, l и s считать новыми буквами, а символ a_0 считать новой *собственной* буквой (для ясности мы будем писать в таком случае a_0'), то мы получим слово над алфавитом

$$\{a_0'\} \cup A_t \cup \{q_0, \ldots, q_n, r, l, s\},$$

если A_t был рабочим алфавитом, а $q_0, \ldots, q_n$—состояниями машины T. Мы будем считать, что это слово и таблица T представляют собой одно и то же. Мы хотим, однако, охарактеризовать T словом из ее рабочего алфавита. Если мы применим к построенному выше слову функцию $\gamma_{t+n+4,\,t}$ (ср. § 3, п. 9), то мы как раз получим слово w над A_t, но при этом мы не сможем по w восстановить таблицу, так как мы не можем без дополнительной информации определить n по w. Только зная пару слов n, w (вспомним о нашей интерпретации целых чисел!), мы можем вновь получить таблицу, используя $\gamma^{-1}_{t+n+4,\,t}$. С помощью σ_2^t (ср. § 3, п. 9) эта пара может быть снова охарактеризована одним словом над A_t. Объединяя эти рассуждения, мы приходим к такому выводу. Пусть T есть некоторая м.Т. с рабочим алфавитом A_t и состояниями $q_0, \ldots, q_n$. Пусть w' есть таблица T. Тогда T может быть однозначно охарактеризована словом

$$w = \sigma_2^t(n, \gamma_{t+n+4, t}(w'))$$

над A_t. При этом w' может быть эффективно найдено по w, а w—эффективно по w'. Помимо этого, можно очевидным образом установить, представляет ли данное слово над A_t некоторую м.Т. или не представляет. Таким образом, мы осуществили гёделизацию (ср. § 1, п. 4) множества всех м.Т. над рабочим алфавитом A_t.

Соответствующее машине T согласно этой гёделизации слово мы будем обозначать через w_T и называть машинным словом T.

2. Одно неразрешимое множество

Мы зададимся алфавитом A_t и рассмотрим множество M слов над A_t, определяемое следующим условием:

$w \in M$ в том и только в том случае, если существует м.Т. T над A_t, для которой $w = w_T$ и которая после применения к w останавливается через конечное число шагов после знака |.

При этом, в частности, для произвольной м.Т. T над A^t

$w_T \in M$ тогда и только тогда, когда T после применения к w_T останавливается через конечное число шагов после знака |.

Мы утверждаем, что M неразрешимо. Это положение вещей можно выразить по-другому, сказав, что вопрос о том, остановится ли после применения к своему машинному слову произвольная наперед заданная м.Т. с рабочим алфавитом A_t через конечное число шагов после знака |, алгоритмически неразрешим.

Доказательство. Предположим, что M разрешимо. Тогда найдется м.Т. T над A_t (без вспомогательных букв!), которая вычисляет χ_M (ср. § 1, п. 6); таким образом, после применения к произвольному слову w над A_t машина T останавливается через конечное число шагов

$$\text{после } \square, \text{ если } w \in M,$$
$$\text{после } |, \text{ если } w \notin M.$$

В частном случае $w = w_T$ мы имеем

> после применения к w_T машина T останавливается через конечное число шагов после $\square$ тогда и только тогда, когда $w_T \in M$, но $w_T \in M$ тогда и только тогда, когда после применения к w_T машина T останавливается через конечное число шагов после | (определение M).

Нужное противоречие достигнуто, так как $| \neq \square$.

3. Другие неразрешимые множества

В этом пункте мы докажем неразрешимость еще двух множеств. Эти множества также тесно связаны с понятием машины Тьюринга, так что вопрос об их неразрешимости вне рамок теории машин Тьюринга представляется малоинтересным. Однако применяемый здесь способ доказательства типичен для методов, с помощью которых устанавливается неразрешимость какого-либо множества. А именно, мы покажем, что разрешимость этих множеств влечет за собой разрешимость множества M из п. 2. Таким образом, эти множества должны быть неразрешимы. Тем же методом доказывается неразрешимость множеств, представляющих интерес и с математической точки зрения (ср., например, статьи Эббинхауза и Хермеса в этой книге).

Пусть задан алфавит A_t. Мы определим множества M_1 и M_2 слов над A_t следующим образом:

$w \in M_1$ в том и только в том случае, если существует м. Т. T над A_t, для которой $w = w_T$ и которая после применения к w останавливается через конечное число шагов;

$w \in M_2$ в том и только в том случае, если существует м. Т. T над A_t, для которой $w = w_T$ и которая после применения к пустой ленте останавливается через конечное число шагов.

В частности, для машинных слов мы, как и в п. 2, имеем

$w_T \in M_1$ в том и только в том случае, когда T после применения к w_T останавливается через конечное число шагов;

$w_T \in M_2$ в том и только в том случае, когда T после применения к пустой ленте останавливается через конечное число шагов.

Множества M_1 и M_2 неразрешимы. Этот факт можно снова выразить в форме, аналогичной использованной в п. 2 для описания неразрешимости [1]).

Доказательство для M_1. Предположим, что M_1 разрешимо. Тогда разрешимо и M.

В самом деле, пусть w — произвольное, но фиксированное слово над A_t. Сначала мы устанавливаем, является ли вообще w машинным словом (согласно п. 1, это может быть выполнено эффективно). Если это не так, то $w \notin M$. Если же это так, то мы восстанавливаем по w соответствующую таблицу (согласно п. 1, это также может быть выполнено эффективно).

Пусть T есть м. Т., соответствующая этой таблице, т. е. $w_T = w$. Теперь мы устанавливаем, имеет ли место принадлежность $w \in M_1$ или нет. Если $w \notin M_1$, то $w \notin M$. Если же, напротив, $w \in M_1$, то мы устанавливаем рабочую ячейку T в начальной позиции после w и пускаем машину. Так как $w \in M_1$, то мы уверены в том, что через конечное число шагов T остановится. Когда это произойдет, мы выясним, остановилась ли T после знака |. Если это так, то $w \in M$, если нет, то $w \notin M$.

Тем самым мы указали процедуру, разрешающую M в интуитивном смысле. Тезис Чёрча гарантирует нам существование и машины Тьюринга, разрешающей M. Можно, однако, избежать применения тезиса Чёрча и прямо скон-

[1]) Эти и подобные утверждения формулируют также как неразрешимость проблемы самораспознаваемости для машин Тьюринга.— *Прим. перев.*

струировать м. Т., моделирующую описанный выше процесс. Существенной составной частью этой машины Тьюринга была бы наряду с м. Т., разрешающей M_1, еще некая универсальная м. Т., аналогичная описанной ниже, в п. 3 § 6. Однако мы должны отказаться от описания здесь такой м. Т., разрешающей M, ввиду ее сложности.

Доказательство для M_2. Мы покажем теперь тем же способом, что разрешимость M_2 влечет за собой разрешимость M_1. Предположим, что M_2 разрешимо, и покажем, что разрешимо M_1.

Пусть выбрано произвольное слово w над A_t. Устанавливаем, является ли w машинным словом. Если не является, то $w \notin M_1$. Если же является, то восстанавливаем по w соответствующую таблицу. Пусть м. Т. с этой таблицей есть T. Пусть, далее, $w = a_{i_1} \ldots a_{i_k}$. Мы рассмотрим машину Тьюринга

$$T' = r a_{i_1} r a_{i_2} \ldots r a_{i_k} r T.$$

Отсюда следует, в частности, что

> T' останавливается после применения к пустой ленте через конечное число шагов тогда и только тогда, когда T останавливается через конечное число шагов после применения к w.

Согласно нашему предположению, мы можем разрешить вопрос о том, останавливается ли T' после применения к пустой ленте через конечное число шагов. Если не останавливается, то $w \notin M_1$, если же останавливается, то $w \in M_1$. Таким образом, мы нашли разрешающую процедуру для M_1.

МАШИНЫ ТЬЮРИНГА И ВЫЧИСЛИМЫЕ ФУНКЦИИ III

Г.-Д. ЭББИНХАУЗ

§ 6. Универсальная машина Тьюринга и теорема Клини о перечислимости

Пусть $A = A_t$ есть какой-то фиксированный алфавит. Далее мы дадим эффективную конструкцию м. Т. U, на которой может быть *промоделирована* (в требующем некоторого уточнения смысле) любая м. Т. с рабочим алфавитом A. Мы назовем U *универсальной* м. Т. для алфавита A. Затем, используя U, мы докажем так называемую *теорему Клини о перечислимости* для в. Т. функций и в дополнение к этой теореме — неразрешимость *проблемы останова* для U. Тем самым мы получим интересный вариант результата из части II, § 5, п. 3. (Использование м. Т. с неразрешимой проблемой останова в статье о перечислимости является существенным моментом в доказательстве неразрешимости арифметики). Нам не хотелось бы оставить без упоминания тот факт, что возможно эффективное задание такой м. Т., которая была бы в состоянии моделировать произвольную машину над *произвольным* алфавитом. Однако это не может быть осуществлено на выбранном нами «прямом» пути; в самом деле, в этом случае символы a_0, a_1, ... должны сами рассматриваться как слова над некоторым фиксированным алфавитом (примерно так, как кодируются обычные буквы в азбуке Морзе), чтобы можно было обойтись конечным числом букв[1]).

1. Универсальная машина Тьюринга U

В основе конструкции U лежит следующая идея. После применения к данной записи в данной ячейке м. Т. T рабо-

---

[1]) Аналогичная конструкция была реализована в п. 10 § 3 и п. 2 § 4. Используя ее, можно дополнить построения настоящего параграфа и получить универсальную машину Тьюринга над произвольным алфавитом. — *Прим. перев.*

тает согласно известным указаниям, извлекаемым из ее таблицы. Это наводит на мысль построить такую м. Т., которая могла бы работать как произвольная данная м. Т. T с рабочим алфавитом A, если только ее таблица помещена на ленту в подходящем виде в качестве дополнительной информации.

Пусть $A' = A_{2t+9}$. Выпишем буквы из множества $A' \setminus A$ в виде следующего ряда символов, наглядный смысл которых станет понятен дальше: $\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_t$, $\boldsymbol{r}$, $\boldsymbol{l}$, $\boldsymbol{s}$, $\boldsymbol{+}$, $\boldsymbol{-}$, $\boldsymbol{O}$, $\boldsymbol{c}$, $\S$. Знаки $\boldsymbol{r}$, $\boldsymbol{l}$, $\boldsymbol{s}$ совпадают с соответствующими обозначениями для действий, но из контекста будет каждый раз понятно, что имеется в виду.

Мы сопоставим каждой м. Т. T с рабочим алфавитом A (точнее, таблице T) *машинное слово* w^T над A', но несколько иным способом, чем это было сделано в § 5. Изменения имеют своей целью упростить описание машины $\boldsymbol{U}$. Для данной таблицы T слово w^T строится эффективно, и, обратно, T может быть эффективно восстановлена по w^T.

Таблица T может быть представлена в форме

$$\begin{matrix} T_0 \\ \vdots \\ T_s \end{matrix}$$

где i-я матрица T_i состоит из строк таблицы T, начинающихся символом q_i ($q_0, \ldots, q_s$ являются состояниями T). Мы сопоставим каждой строке $q_i a_j v_{ij} q_{k_{ij}}$ таблицы T следующее слово:

$$w_{ij}^T = \begin{cases} \boldsymbol{b}_j v_{ij} \boldsymbol{+}^{k_{ij}-i}, & \text{если } k_{ij} > i, \\ \boldsymbol{b}_j v_{ij} \boldsymbol{O}, & \text{если } k_{ij} = i, \\ \boldsymbol{b}_j v_{ij} \boldsymbol{-}^{i-k_{ij}}, & \text{если } k_{ij} < i. \end{cases}$$

Заключительная часть слова w_{ij}^T, следующая за символом v_{ij}, представляет в наглядной форме разность индексов следующего и исходного состояний. Матрице T_i сопоставляется слово

$$w_i^T = w_{i0}^T \ldots w_{it}^T$$

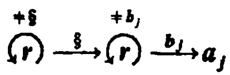
и, наконец, всей таблице T — слово

$$w^T = \boldsymbol{c} w_0^T \boldsymbol{c} \ldots \boldsymbol{c} w_s^T \S.$$

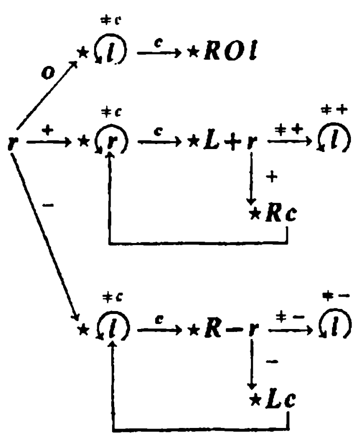
Пусть l_T — длина w^T. Для каждого $i=0, \ldots, s$ мы получим из w^T слово $w^T(q_i/\bigstar)$, заменив символ c, находящийся непосредственно перед частью w_i^T, символом $\bigstar$. Слово $w^T(q_i/\bigstar)$ является несобственным. Так же как и w^T, оно является эффективным представлением T и при этом с отмеченным состоянием q_i.

Пусть рабочий алфавит U есть A'. Мы зададим U с помощью диаграммы.

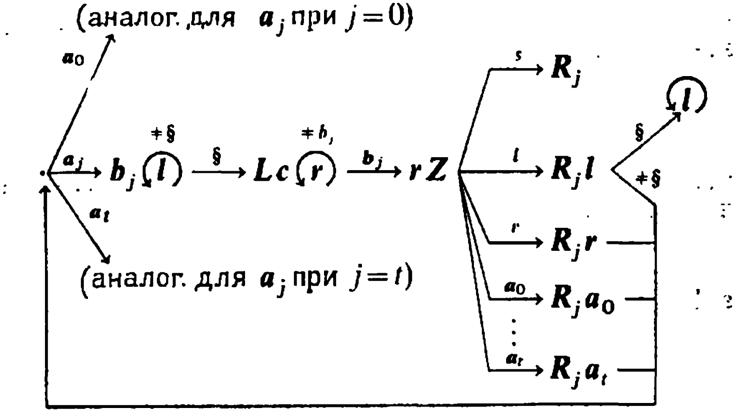
Для каждого $j=0, \ldots, t$ пусть R_j обозначает м. Т. с диаграммой



и пусть Z обозначает м. Т. с диаграммой



Определим машину U следующей диаграммой:



Мы опишем порядок работы U для случая, когда U моделирует некоторую м. Т. T с рабочим алфавитом A; далее мы ближе познакомимся с тем, что понимается здесь под моделированием. Порядок работы U в иных ситуациях нас здесь не интересует.

Сначала мы сопоставим каждой конфигурации

$$C=(m,\ \mathfrak{J},\ q)=a_0\dots a_m^q\dots$$

машины T конфигурацию

$$\bar{C}=(m+l_T,\ \mathfrak{J}_C,\ q_0)=w^T(q/\bigstar)\,a_0\dots a_m^{q_0}\dots$$

машины U. (Таким образом, $\mathfrak{J}_C$ определяется соотношениями

$$\mathfrak{J}_C(0)\dots\mathfrak{J}_C(l_T-1)=w^T(q/\bigstar),\quad \mathfrak{J}_C(j+l_T)=\mathfrak{J}(j)\quad (j\geqslant 0).)$$

Если T применяется к записи $\mathfrak{J}_0$ в рабочей ячейке m_0, то тем самым начальная конфигурация есть $C_0=(m_0,\ \mathfrak{J}_0,\ q_0)$. При моделировании T машина U применяется к записи $\mathfrak{J}_{C_0}$ в рабочей ячейке m_0+l_T; таким образом, в качестве начальной конфигурации выбрана $D_0:=\overline{C}_0$. Очевидно, что если

$$a_0\dots a_{m_0}\dots$$

есть начальная позиция T, то для U выбирается начальная позиция

$$w^T(q_0/\bigstar)\,a_0\ldots\underset{\uparrow}{a_{m_0}}\ldots\,.$$

Чтобы представить себе, каким образом U моделирует машину T, мы предположим, что T в процессе вычислений пришла к конфигурации

$$C=(m,\ \mathfrak{Z},\ q)=a_0\ldots a_m^q\ldots\,,$$

а U — к конфигурации

$$\bar{C}=(m+l_T,\ \mathfrak{Z}_C,\ q_0)=w^T(q/\bigstar)\,a_0\ldots a_m^{q_0}\ldots\,.$$

(Это соответствует началу вычислений!) Пусть

$$qa_mvq'$$

есть строка таблицы T, начинающаяся символами qa_m.

Случай a). $v=s$.

Машинный останов T. При этом C есть конечная конфигурация и

$$a_0\ldots\underset{\uparrow}{a_m}$$

есть конечная позиция T.

Случай b). $v=l$ и $m=0$.

Уход за пределы ленты. Конечная конфигурация T есть C, а конечная позиция

$$\underset{\uparrow}{a_0}\ldots\,.$$

Случай c). Не выполняется ни a), ни b).

У C есть непосредственно следующая за ней конфигурация

$$C'=(m',\ \mathfrak{Z}',\ q')=a'_0\ldots a'^{q'}_{m'}\ldots\,.$$

Что делает U при конфигурации $\bar{C}$? Конфигурации $\bar{C}$ соответствует позиция

$$w^T(q/\bigstar)\,a_0\ldots\underset{\uparrow}{a_m}\ldots\,.$$

Так как состояние $\bar{C}$ есть q_0, то работа начинается с точки на диаграмме U. Пусть, например, $a_m=\mathfrak{a}_j$. Сначала U

печатает b_j на месте a_j, разыскивает с помощью

$$\overset{\neq \S}{\circlearrowleft l} \xrightarrow{\S} Lc$$

знак $\bigstar$ в слове $w^T(q/\bigstar)$ и заменяет его буквой c. Текущая позиция в этот момент (если, например, $q = q_p$) выглядит так:

$$c w_0^T c \ldots c w_{p-1}^T \underset{\uparrow}{c} w_p^T c \ldots c w_s^T \S a_0 \ldots a_{m-1} b_j a_{m+1} \ldots .$$

С помощью

$$\overset{\neq b_j}{\circlearrowleft r}$$

U разыскивает в слове w_p^T, находящемся непосредственно справа от рабочей ячейки, букву b_j. Это приводит к позиции

$$\sim c w_{p1}^T \ldots w_{pj-1}^T \underset{\uparrow}{b_j} v \ldots .$$

Затем U с помощью r сдвигается на одну ячейку вправо. Содержимое v этой ячейки определяет действие, которое должно быть выполнено машиной T при конфигурации C. Следующей должна работать машина Z, которая, как легко проверить, превращает текущую начальную часть w^T записи (ведь знак $\bigstar$ в $w^T(q'/\bigstar)$ заменен буквой c) в слово $w^T(q'/\bigstar)$. (Мы оставляем читателю соответствующие выкладки.) После выполнения этой задачи U снова находится в ячейке, содержащей символ v действия, которое должна выполнять машина T. С помощью R_j машина U вновь разыскивает теперь — независимо от действия v — исходную рабочую ячейку конфигурации $\bar{C}$ и заменяет находящийся в ней символ b_j символом $a_j (= a_m)$. Получившаяся позиция имеет вид

$$w(q'/\bigstar) a_0 \ldots \underset{\uparrow}{a_m} \ldots .$$

Для того чтобы выяснить, как работает U дальше, мы будем различать три возможности:

(1) Случай а) (т. е. $v = s$).

Происходит машинный останов U; конечная позиция есть

$$w(q'/\bigstar)\, a_0 \ldots \underset{\uparrow}{a_m} \ldots .$$

(2) Случай b) (т. е. $v = l$ и $m = 0$).

С помощью l машина U сдвигается на одну ячейку влево, обнаруживает знак § (последнюю букву слова $w(q'/\bigstar)$) и уходит за пределы ленты с помощью

$$\textcircled{l}$$

Конечная позиция имеет вид

$$\underset{\uparrow}{w}(q'/\bigstar)\, a_0 \ldots .$$

(3) Случай c).

U выполняет действие v и переходит (так же как и T) в позицию

$$w(q'/\bigstar)\, a'_0 \ldots \underset{\uparrow}{a'_{m'}} \ldots .$$

Так как в заключение, согласно диаграмме U, должна «работать» точка, то U оказывается теперь в состоянии q_0. Таким образом, U переходит к конфигурации

$$w(q'/\bigstar)\, q'_0 \ldots a'^{q_0}_{m'} = \bar{C}'.$$

Итак, можно следующим образом описать порядок работы U и тем самым уточнить представление о моделировании T машиной U:

6.1. Пусть $C_0, C_1, \ldots$ есть последовательность конфигураций T с начальной конфигурацией C_0, и пусть $D_0, D_1, \ldots$ есть последовательность конфигураций U с начальной конфигурацией $D_0 = \bar{C}_0$. Тогда найдется подпоследовательность $D_{n_0}, D_{n_1}, \ldots$ последовательности $D_0, D_1, \ldots$, имеющая ту же длину, что и последовательность $C_0, C_1, \ldots$ (и, следовательно, вместе с этой последовательностью обрывающаяся либо бесконечная), и обладающая следующими свойствами:

(i) $D_{n_i} = \bar{C}_i \quad (i = 0, 1, \ldots)$.

(ii) Если последовательность $C_0, C_1, \ldots$ обрывается на C_k, то найдется такое r, что последовательность D_0,

$D_1, \ldots$ обрывается на D_{n_k+r}. Пусть, кроме того,

$$\underset{\uparrow}{a_0 \ldots a_m}$$

есть конечная позиция T. Если имеет место машинный останов T, то имеет место и машинный останов U, причем конечной позицией U является при некотором q позиция

$$w^T (q/\bigstar)\, a_0 \ldots \underset{\uparrow}{a_m} \ldots .$$

Если T уходит за пределы ленты (в этом случае, в частности, $m = 0$), то U также уходит за пределы ленты и конечной позицией U является при некотором q позиция

$$\underset{\uparrow}{w^T} (q/\bigstar)\, a_0 \ldots .$$

Отметим еще без доказательства свойство

(iii) Последняя буква § слова w^T не стирается и не печатается машиной U. Конфигурации D_{n_i} в точности соответствуют каждой второй из тех конфигураций из последовательности $D_0, D_1, \ldots$, рабочие ячейки которых находятся правее ячейки, занятой символом §, и все ячейки правее этой последней ячейки заняты только буквами из алфавита $A \cup \{a_0\}$; при этом упомянутые конфигурации из последовательности $D_0, D_1, \ldots$ суть те и только те конфигурации, состояние которых есть q_0.

Из 6.1 следует, в частности, что если C_0 — начальная конфигурация машины T, а $D_0 = C_0$ — начальная конфигурация машины U, то

6.2. (1) T останавливается в том и только в том случае, если останавливается U.

(2) Машинный останов T происходит в том и только в том случае, если происходит машинный останов U.

(3) T останавливается после некоторого слова $w \in \Omega(A)$ (!) в том и только в том случае, если U останавливается после w.

В качестве следствия сформулируем такое предложение:

6.3. Теорема. *Можно эффективно построить для алфавита A универсальную машину Тьюринга,*

2. Теорема Клини о перечислимости для вычислимых по Тьюрингу функций

Используя универсальную м. Т. U, мы докажем здесь следующую теорему, принадлежащую Клини (ср. Клини [6], стр. 272):

6.4. Теорема. *Для любого n найдется в. Т. функция F из $\Omega^{n+1}(A)$ в $\Omega(A)$, для которой функции f_w, определяемые равенством $f_w(\mathfrak{w}) \cong F(w, \mathfrak{w})$ $(\mathfrak{w} \in \Omega^n(A))$, пробегают всю совокупность (и только ее) в. Т. функций из $\Omega^n(A)$ в $\Omega(A)$, когда w пробегает $\Omega(A)$.*

Такая функция F называется *универсальной* функцией для числа переменных n. Если $f = f_w$, то w называют *индексом* или *гёделевским номером* f относительно F. Так как в. Т. функция из $\Omega^n(A)$ в $\Omega(A)$ может быть вычислена бесконечным числом м. Т. над A, то, как можно заключить из нижеследующего доказательства, она обладает бесконечным количеством индексов относительно F.

При доказательстве теоремы 6.4 мы будем руководствоваться следующим соображением. В. Т. функция f из $\Omega^n(A)$ в $\Omega(A)$ может быть вычислена машиной U, если на ленте, помимо аргумента, имеется еще и нужная информация, которая позволит промоделировать на U вычисляющую f машину T с рабочим алфавитом A. Эта информация в основном совпадает с машинным словом w^T. Тогда F есть функция, которая в главных чертах определяется этой машиной U и первый аргумент которой, очевидно, является таким носителем информации.

Пусть F' есть в. Т. функция из $\Omega^{n+1}(A')$ в $\Omega(A)$, определяемая машиной U, и пусть γ обозначает взаимно однозначную в. Т. функцию на $\Omega(A)$ со значениями на $\Omega(A')$, определенную в части II, § 3, п. 9. Построим теперь функцию F из $\Omega^{n+1}(A)$ в $\Omega(A)$:

$$F(w, \mathfrak{w}) \cong F'(\gamma(w), \mathfrak{w}) \qquad ((w, \mathfrak{w}) \in \Omega^{n+1}(A)).$$

Так как подстановка в. Т. функций в в. Т. функции приводит снова к в. Т. функциям, то F будет в. Т. функцией. Одновременно F удовлетворяет и условию теоремы 6.4: для каждого $w \in \Omega(A)$ функция f_w, очевидно, также будет в. Т. функцией. (Мы предоставляем читателю проведение всех необходимых здесь рассуждений.) Обратно, пусть f есть в. Т. функция из $\Omega^n(A)$ в $\Omega(A)$. Согласно § 4, существует м. Т. T над алфавитом A, вычисляющая f. Обозначим слово, полученное из w^T зачеркиванием первой буквы c, через $'w^T$. Предположим, что $w \in \Omega(A)$ выбрано таким образом, что $\gamma(w) = {}'w^T$, и пусть $\mathfrak{w} = (w_1, \ldots, w_n) \in \Omega^n(A)$.

Применить T к $\mathfrak{w}$ означает выбрать в качестве начальной конфигурацию

$$C_0 = \bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar^{q_0} \bigstar \ldots .$$

Ввиду того что $\bigstar\, 'w^T = w^T(q_0/\bigstar)$, для $\bar{C}_0$ получается следующее представление:

$$\bar{C}_0 = \bigstar\, 'w^T \bigstar w_1 \bigstar \ldots \bigstar w_n \bigstar^{q_0} \bigstar \ldots .$$

Выбрать $\bar{C}_0$ в качестве начальной конфигурации для U означает, таким образом, применить U к $('w^T, \mathfrak{w})$. Согласно 6.2(3), отсюда следует, что T останавливается после применения к $\mathfrak{w}$ после некоторого слова w' над A тогда и только тогда, когда U после применения к $('w^T, \mathfrak{w})$ останавливается после w'.

Это приводит к равенству

$$f(\mathfrak{w}) \cong F'('w^T, \mathfrak{w}).$$

Из равенств

$$F'('w^T, \mathfrak{w}) \cong F'(\gamma(w), \mathfrak{w}) \cong F(w, \mathfrak{w}) \cong f_w(\mathfrak{w})$$

следует

$$f = f_w,$$

что и требовалось доказать.

Так как мы можем эффективно задать машины Тьюринга, вычисляющие γ и F', то мы можем также эффективно задать и м. Т., вычисляющую (и даже нормированно вычисляющую) функцию F. В этом смысле функция F из 6.4 может быть задана *эффективным образом*.

3. Проблема останова для U

Из рассмотрений п. 1 можно извлечь также еще одно следствие: *неразрешимость проблемы останова для U*. Мы дадим здесь лишь набросок доказательства. Впрочем, нетрудно было бы развить наши рассуждения и сделать их применимыми к уточненным по Тьюрингу понятиям. (Если принят тезис Чёрча, то в этом нет необходимости.)

6.5. Теорема. *Множество*

$$M = \{\mathfrak{w} : \mathfrak{w} \in \Omega(A') \text{ и } U \text{ после применения к } \mathfrak{w} \text{ останавливается}\}$$

неразрешимо; это означает, что не существует никакого правила, с помощью которого можно было бы для произвольного слова $\mathfrak{w}$ над A' установить, останавливается ли U после применения к $\mathfrak{w}$.

Будем рассуждать от противного. Пусть M разрешимо. Так как множество слов над A' вида $'\mathfrak{w}^T$ (T есть некоторая м. Т. с рабочим алфавитом A) разрешимо, то множество

$$\{'\mathfrak{w}^T : T \text{ есть м. Т. с рабочим алфавитом } A \text{ и } U \text{ останавливается после применения к } '\mathfrak{w}'\}$$

также разрешимо. Так как для конфигурации

$$C_0 = \bigstar \bigstar^{q_0} \bigstar \ldots$$

некоторой м. Т. T с рабочим алфавитом A конфигурация $\bar{C}_0$ имеет вид

$$\bar{C}_0 = \bigstar\, '\mathfrak{w}^T \bigstar \bigstar^{q_0} \bigstar \ldots,$$

то, согласно 6.2(1), разрешим вопрос о том, останавливается ли произвольная м. Т. с рабочим алфавитом A после применения к пустой ленте. Но это противоречит утверждению п. 3 § 5 части II.

ЛИТЕРАТУРА

1. Church A., An Unsolvable Problem of Elementary Number Theory, *Amer. J. Math.*, **58** (1953), 345—363.
2. Davis M., Computability and Unsolvability, New York—Toronto—London, McGraw-Hill, 1958.
3. Gödel K., Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I, *Monatsch. Math. Phys.*, **38** (1931), 173—198.
4. Hermes H., Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit, Berlin—Göttingen—Heidelberg, Springer, 1961.
5. Kalmár L., An Argument Against the Plausibility of Church's Thesis, In: Heiting A. (Ed.), Constructivity in Mathematics, 72—80, Amsterdam, North-Holland Publishing Co., 1959.

6. Клини С. К., Введение в метаматематику, ИЛ, М., 1957.
7. Péter R., Rekursivität und Konstruktivität, In: Heiting A. (Ed.), Constructivity in Mathematics, 226–233, Amsterdam, North-Holland Publishing Co., 1959.
8. Post E. L., Finite Combinatory Processes — Formulation I, *J. Symb. Log.*, **1** (1936), 103—105.
9. Rogers H., Theory of Recursive Functions and Effective Computability, New York — St. Louis — San Francisco, McGraw-Hill, 1967.
10. Turing A. M., On Computable Numbers with an Application to the Entscheidungsproblem, *Proc. Lond. Math. Soc.* (ser. 2), **42** (1936/37), 230—265, and **43** (1937), 544—546.
11*. Robinson J., Existential definability in arithmetic, *Trans. Amer. Math. Soc.*, **72** (1952), 437—449.
12*. Дэвис М., Путнам Х., Робинсон Дж., Проблема разрешимости для показательно-диофантовых уравнений, сб. *Математика*, **8**:5 (1964), 69—79.
13*. Матиясевич Ю. В., Диофантовость перечислимых множеств, *ДАН СССР*, **191**, № 2 (1970).

ПЕРЕЧИСЛИМОСТЬ

Г.-Д. ЭББИНХАУЗ

§ 1. Введение

1. Интуитивное представление о перечислимости. Обзор содержания

Вряд ли у кого-нибудь возникнут сомнения в том, что любой школьник, знакомый с основами теории чисел, может — по крайней мере в принципе — вычислить все простые числа до произвольной заранее указанной границы и что причины, которые могут ему помешать проделать это на практике, никак не связаны с простыми числами, а имеют медико-биологическую или физико-техническую природу. В основе нашей уверенности лежит предположение, что любому школьнику известна *процедура* выделения простых чисел, скажем, в десятичной записи и занесения их в список в порядке возрастания и что не существует — по крайней мере в принципе — никаких ограничений для ее реализации. Мы говорим, что *множество простых чисел перечислимо*. Метод выделения и записи простых чисел мы называем *перечислительной процедурой*.

Дальше мы познакомимся с некоторыми основными проблемами и результатами теории перечислимых множеств. Но сначала сосредоточим наши усилия на уточнении интуитивного представления о перечислимости.

Для того чтобы какой-то объект мог быть элементом перечислимого множества и тем самым — объектом некоторого процесса перечисления, он должен быть доступен определенному воздействию, т. е. должен быть конструктивным.

В предыдущей статье о машинах Тьюринга и вычислимых функциях (для ссылок на нее мы будем в дальнейшем использовать сокращение МТВФ) были высказаны соображения, согласно которым при изучении множеств конструктивных элементов мы можем ограничиться рассмотрением множеств n-членных последовательностей слов над некоторыми алфавитами. Для таких множеств мы можем сформулировать все еще интуитивное, но уже более точное

1.1. Определение. Некоторое множество $\mathfrak{M}$ n-членных последовательностей слов над каким-то алфавитом называется *перечислимым* в том и только том случае, когда существует общая процедура, с помощью которой могут быть систематическим образом получены все элементы $\mathfrak{M}$. Эта общая процедура называется *перечислительной процедурой* для $\mathfrak{M}$.

Мы не требуем (и хотели бы это особенно подчеркнуть), чтобы для всякого перечислимого множества можно было бы эффективно указать перечислительную процедуру; квантор существования в 1.1 следует понимать,— как и при определении вычислимых функций (ср. МВТФ I, 1.9), — в *классическом* смысле. (На практике, однако, доказательства перечислимости множеств будут, как правило, состоять в *эффективном* задании перечислительной процедуры.)

Приведем некоторые примеры перечислимых множеств.

1.2. Пустое множество.

Перечислительная процедура может, например, сводиться к предписанию: не разрешается ничего выписывать.

1.3. Множество слов над алфавитом $\{|\}$, содержащих четное число штрихов.

Перечислительная процедура дается следующим предписанием: пишут пустое слово; если некоторое слово выписано, то следующим пишут слово, отличающееся от первого двумя дополнительными штрихами.

1.4. Множество слов над некоторым алфавитом A. Мы укажем две перечислительные процедуры для этого множества со следующими предписаниями:

(1) Сначала пишут пустое слово; если выписано слово w длины l, то дальше пишут слово длины l над A, лексикографически непосредственно следующее за w, если w — не (лексикографически) последнее слово длины l над A; в противном случае пишут лексикографически первое слово над A длины $l+1$.

(2) Пишут пустое слово; далее пишут слово, получающееся из какого-то уже выписанного слова добавлением одной буквы из A.

Эти примеры дают первое, и если быть скромными, то весьма приблизительное представление о том, что может скрываться за появившимися в 1.1 нестрогими формулировками «общая процедура» и «возможность систематического получения».

При уточнении этих понятий мы сталкиваемся с трудностями, аналогичными возникшим в МТВФ I при уточнении понятий алгоритма и вычислимых функций. Мы попытаемся преодолеть эти трудности следующим образом. Мы покажем в § 2, что существует тесная связь между понятиями вычислимости и перечислимости, и ввиду этого любое уточнение одного из этих понятий приводит к уточнению другого. Из полученного в МТВФ I, § 2, уточнения понятия вычислимости с помощью *машин Тьюринга* мы построим точное определение *перечислимости по Тьюрингу.*

Мы предпошлем нашим рассмотрениям предположение, что для каждого перечислимого множества найдется перечислительная процедура, удовлетворяющая условиям, сформулированным в МТВФ I, 1.1—1.8, для алгоритмов, в частности, однозначно и поэтапно выполнимая, как это имеет место в примерах 1.2, 1.3 и 1.4(1). Тезис Чёрча, в силу которого понятие вычислимости по Тьюрингу являлось адекватным уточнением интуитивного представления о вычислимости, утверждает также и в этом случае, что при таком предположении *понятие перечислимости по Тьюрингу есть адекватное уточнение интуитивного представления о перечислимости.*

Ближе мы познакомимся с перечислимыми по Тьюрингу множествами в § 3. Там же мы установим факт существования так называемых *универсальных* перечислимых по Тьюрингу множеств (*теорема о перечислимости Клини*, [10]) и дадим примеры «конкретных» не перечислимых по Тьюрингу множеств.

Если при попытке уточнить интуитивные представления мы будем исходить не из одних лишь однозначно выполнимых перечислительных процедур, то перед нами откроется другой, не использующий определения вычислимой функции подход к анализу понятия перечислимости — через так называемые *исчисления*, или *системы правил вывода.*

Примером процедуры, выполнение которой не обязательно приводит к однозначно определенной последовательности выделенных ею элементов какого-то множества, является 1.4(2). Часто проводят различие между перечислительными процедурами однозначного и не обязательно однозначного действия. Так как с интуитивной точки зрения во втором случае на передний план выступает не *перечислительный* аспект процедуры, а скорее ее *креативный* (творческий) аспект, то при этом, следуя Посту [13], говорят о *креативных* (порожденных) множествах. Здесь же мы не будем делать такого различия, а будем просто говорить о *перечислительных* процедурах и *перечислимых* множествах.

В § 4 мы вводим исчисления, а затем, используя специальное исчисление, так называемую *формальную систему Шмульяна* [15], приходим, наконец, к формулировке еще одного точного понятия перечислимости — *перечислимости по Шмульяну*. Поскольку мы не исследуем понятие исчисления с интуитивной точки зрения так подробно, как мы исследовали понятие алгоритма в МТВФ I, то, вообще говоря, совсем не очевидно, что формальная система Шмульяна является адекватным уточнением понятия исчисления, а перечислимость по Шмульяну — адекватным уточнением понятия перечислимости. Впрочем, мы сумеем привести некоторые аргументы в пользу такой адекватности, установив в § 5, что всякое перечислимое по Тьюрингу множество перечислимо по Шмульяну, и дав набросок доказательства обратного утверждения.

В § 6 мы покажем, что одно особенно интересное для математиков множество — *множество истинных арифметических высказываний*, — *неперечислимо*. Следствием этого факта является теорема о неразрешимости арифметики (Тарский [16]): не существует алгоритма, с помощью которого можно было бы для произвольного наперед заданного арифметического утверждения за конечное число шагов решить, истинно оно или нет.

Мы пользуемся обозначениями, введенными в МТВФ. Особенно часто мы ссылаемся на МТВФ I, п. 3, § 1. В § 3 и 5 мы используем, кроме того, ряд теорем о машинах Тьюринга и вычислимых по Тьюрингу функциях, которые можно найти, например, в МТВФ II. Употребляемая там терминология была введена в МТВФ I, § 2.

2. Исторические замечания

В результате быстрого развития алгоритмических методов, особенно в арабском мире, в XIII столетии возникло желание найти какую-то *формальную схему получения всех истинных высказываний*. Первой неполной, но богатой по своим духовным историческим последствиям попыткой была книга «Ars magna» («Могущественная наука») испанца *Раймонда Люллю* (около 1235—1315 г.).

Лейбниц придал этим замыслам более ясную и современную форму. Вот что, между прочим, писал юный Лейбниц около 1671 г. тогдашнему герцогу Брауншвейгскому-Люнебургскому (ср. Герхард [6], стр. 57):

«...В философии мною найдено средство достичь того же, что сделали Декарт и другие для арифметики и геометрии с помощью алгебры и анализа, но уже для всех наук *per Artem Combinatoriam*[1]); она разрабатывалась еще Люллю и П. Кирхером, которые, однако, не смогли проникнуть в ее суть. Тем самым указан путь, на котором все существующие на свете составные понятия могут быть разложены на небольшое число простых понятий, являющихся как бы их алфавитом, и посредством правильного метода из комбинаций букв такого алфавита могут быть со временем вновь получены все вещи вместе с их теоретическими доказательствами. Это открытие, если только Бог судил мне его закончить, было бы матерью всех моих открытий и чрезвычайно важным само по себе...».

Вопреки первому утверждению этой цитаты Лейбницу не было суждено достичь успеха. Заслуга осуществления его идей принадлежит в первую очередь *Фреге*, *Расселу* и *Гёделю* (теорема Гёделя о *полноте* логики предикатов первой ступени, ср. Гёдель [7]). *Доказательство неосуществимости* программы Лейбница в рамках логики предикатов второй ступени также является достижением Гёделя (Гёдель [8]). Доказательство неперечислимости множества истинных арифметических высказываний из § 6

---

[1]) Посредством Комбинаторики (или Искусства формул) (*лат.*). Яркое изложение идей Лейбница можно найти в книге Н. Бурбаки [18], стр. 14—17.— *Прим. перев.*

может в этой связи рассматриваться как доказательство невыполнимости этой программы в рамках построенного в § 6 языка арифметики.

Основы общей теории перечислимых множеств были заложены Постом [13]. Ныне она выросла в важную область так называемой *рекурсивной теории*. Вопросы перечислимости играют также значительную роль в теории *формальных языков* и *математической лингвистике* (ср. Хомский [2], Хомский и Миллер [3]).

§ 2. Простые теоремы о перечислимых множествах

1. Предварительные замечания

Наша цель — дать «наивное» доказательство того факта, что понятие вычислимости может быть сведено к понятию перечислимости, и наоборот. Второе сведение дает нам возможность положить в основу формализации понятия перечислимости понятие вычислимости. Это и будет сделано в 3.1 при определении перечислимости по Тьюрингу.

В дальнейших рассуждениях используются лишь самые поверхностные представления о вычислительных и перечислительных процедурах, хотя мы и предполагаем, что рассматриваемые перечислительные процедуры удовлетворяют известным условиям (например, однозначной выполнимости). Для понимания дальнейшего необходимо принять во внимание следующее. Для того чтобы уточнить понятие вычислимости с помощью машин Тьюринга, мы выдвинули в МТВФ I целый ряд требований к допустимым алгоритмам. Если мы хотим теперь использовать приведенную ниже теорему 2.2 для того, чтобы свести проблему уточнения понятия перечислимости к понятию вычислимости, то нам необходима уверенность в том, что теорема 2.2 выполняется и в тех случаях, когда допускаются лишь такие вычислительные процедуры, которые удовлетворяют этим требованиям. Это возможно лишь тогда, когда и перечислительные процедуры удовлетворяют соответствующим требованиям (например, поэтапной выполнимости).

Можно было бы теперь, как и в МТВФ I, предпринять анализ понятия перечислимости с интуитивной точки зрения и показать на примерах, что класс перечислимых множеств не будет обеднен введением соответствующих требований к перечислительным процедурам. Однако нам хотелось бы избежать этого, иначе наши подготовительные рассуждения чрезмерно разрастутся.

2. Сведение понятия вычислимости к понятию перечислимости

Определим график функции f как множество $\mathrm{Graph}\, f := \{(\mathfrak{w}, f(\mathfrak{w})) : \mathfrak{w} \in \mathrm{Def}\, f\}$ (по поводу обозначений $\mathrm{Def}\, f$, $\mathrm{Bild}\, f$ и т. д. см. МТВФ I, п. 5 § 1).

2.1. Теорема. *Пусть $n \geqslant 1$ и f есть некоторая функция из $\Omega^n(E)$ в $\Omega(B)$. Функция f вычислима в том и только в том случае, когда множество $\mathrm{Graph}\, f$ перечислимо.*

Доказательство. Предположим сначала, что функция f вычислима. Пусть $\mathfrak{V}_f$ есть какая-то вычислительная процедура для f. Мы можем указать следующую схему получения элементов $\Omega^n(E)$: для всех $k = 0, 1, \ldots$ перенумеруем все лексикографически упорядоченные слова из $\Omega(E \cup \{,\})$ длины k и оставим только те слова, которые содержат равно $n-1$ запятых. Обозначим эту процедуру через $\mathfrak{V}$. Для того чтобы перенумеровать элементы множества $\mathrm{Graph}\, f$ числами ряда $k = 1, 2, \ldots$, мы будем действовать следующим образом: используя $\mathfrak{V}$, получим первые k элементов $\mathfrak{w}_1, \ldots, \mathfrak{w}_k$ из $\Omega^n(E)$ и выполним с каждым из них k первых шагов процедуры $\mathfrak{V}_f$, пока это возможно: если при этом $\mathfrak{V}_f$, примененная к какому-то элементу $\mathfrak{w}_i$, обрывается после максимального числа k шагов с результатом w_i, то $(\mathfrak{w}_i, w_i)$ есть один из полученных нами на этом этапе элементов $\mathrm{Graph}\, f$. Каждый элемент множества $\mathrm{Graph}\, f$ будет в конце концов получен таким образом.

Обратно, пусть множество $\mathrm{Graph}\, f$ перечислимо и $\mathfrak{V}$ есть процедура систематического получения элементов $\mathrm{Graph}\, f$. Следующая процедура будет тогда вычислительной процедурой для функции f:

Пусть задано $\mathfrak{w} \in \Omega^n(E)$. Выполняем процедуру $\mathfrak{V}$ систематического перечисления элементов $\mathrm{Graph}\, f$ и для каждого вновь полученного элемента сравниваем его первые n компонент с соответствующими компонентами $\mathfrak{w}$. Когда эти компоненты впервые совпадут, процедуру вычисления $f(\mathfrak{w})$ обрываем с результатом, равным $(n+1)$-й компоненте соответствующего элемента $\operatorname{Graph} f$. Если процедура $\mathfrak{V}$ оборвется прежде, чем это произойдет, то обрываем и вычислительную процедуру для $f(\mathfrak{w})$ и считаем, что она не имеет результата.

3. Редукция понятия перечислимости к понятию вычислимости

2.2. Теорема. *Пусть* $n \geqslant 1$ *и* $\mathfrak{M} \subset \Omega^n(A)$. *Множество* $\mathfrak{M}$ *перечислимо тогда и только тогда, когда существуют алфавит* E *и вычислимые функции* $f_1, \ldots, f_n$ *из* $\Omega(E)$ *в* $\Omega(A)$, *такие, что*

$$\mathfrak{M} = \left\{(f_1(w), \ldots, f_n(w)) : w \in \bigcap_{i=1}^{n} \operatorname{Def} f_i\right\}.$$

(В частности, при $n=1$ теорема 2.2 утверждает, что $\mathfrak{M}$ перечислимо в том и только в том случае, когда $\mathfrak{M}$ есть область значений некоторой вычислимой функции.)

Доказательство. Предположим сначала, что $\mathfrak{M}$ перечислимо. Пусть $\mathfrak{V}$ есть некоторая перечислительная процедура для $\mathfrak{M}$, которая упорядочивает элементы $\mathfrak{M}$ в виде *однозначно определенной последовательности*. Мы определим искомые вычислимые функции $f_1, \ldots, f_n$ из $\mathbf{N}$ в $\Omega(A)$ с помощью следующей вычислительной процедуры. Пусть задано $m \in \mathbf{N}$. Выполняем $\mathfrak{V}$ до тех пор, пока не получим m-й элемент $\mathfrak{M}$. Если $\mathfrak{V}$ обрывается раньше, то обрываем и процедуру, считая, что она не имеет результата. В противном случае считаем i-ю компоненту m-го элемента $\mathfrak{M}$ значением функции $f_i(m)$ $(1 \leqslant i \leqslant n)$.

Предположим теперь для доказательства обратного утверждения, что имеется алфавит E и вычислимые функции $f_1, \ldots, f_n$ из $\Omega(E)$ в $\Omega(A)$, такие, что

$$\mathfrak{M} = \left\{(f_1(w), \ldots, f_n(w)) : w \in \bigcap_{i=1}^{n} \operatorname{Def} f_i\right\}.$$

Согласно 2.1, множество $\operatorname{Graph} f_i$ перечислимо для всех $i \in \{1, \ldots, n\}$. Пусть $\mathfrak{V}_i$ есть поэтапно выполнимая перечислительная процедура для множества $\mathrm{Graph}\, f_i$ ($i \in \in \{1, \ldots, n\}$). Теперь можно следующим образом перечислить $\mathfrak{M}$. Приступаем к выполнению $\mathfrak{B}_1, \ldots, \mathfrak{B}_n$, чередуя отдельные шаги этих процедур. Всякий раз, когда некоторая процедура $\mathfrak{B}_j$ имеет своим результатом элемент $(w, w_j) \in \mathrm{Graph}\, f_j$, проверяем, имеются ли среди результатов всех остальных процедур $\mathfrak{B}_i$ элементы вида $(w, w_i) \in \mathrm{Graph}\, f_i$ (в этом случае все w_i однозначно определены). Если это так, то $(w_1, \ldots, w_n)$ и будет как раз элементом $\mathfrak{M}$, полученным таким образом. Если какие-то, но не все из этих процедур обрываются, то опускаем их, если же обрываются все процедуры, то обрываем нашу процедуру.

Задача. Пусть $n=1$ и $\mathfrak{M}$ есть бесконечное перечислимое подмножество $\Omega(A)$. Показать, что существует взаимно однозначная вычислимая функция f, отображающая $\mathbf{N}$ в $\Omega(A)$, для которой $\mathrm{Bild}\, f = \mathfrak{M}$. (Предполагается, что $\mathfrak{M}$ перечислимо «без повторений».)

4. Перечислимость и разрешимость

Понятия перечислимости и разрешимости тесно связаны, что видно из следующей теоремы[1]):

2.3. Теорема. *Пусть $n \geqslant 1$ и $\mathfrak{M} \subset \Omega^n(A)$. Множество $\mathfrak{M}$ разрешимо тогда и только тогда, когда перечислимы $\mathfrak{M}$ и $\Omega^n(A) \setminus \mathfrak{M}$.*

Доказательство. Мы знаем, что $\Omega^n(A)$ перечислимо. Предположим сначала, что $\mathfrak{M}$ разрешимо. Опишем вкратце перечислительную процедуру для $\mathfrak{M}$ (аналогичная процедура строится и для $\Omega^n(A) \setminus \mathfrak{M}$). Перечисляем элементы $\Omega^n(A)$. Для очередного перечисляемого элемента проверяем, принадлежит ли он $\mathfrak{M}$. Те элементы, которые не принадлежат $\mathfrak{M}$, отбрасываем.

Предположим теперь, что $\mathfrak{M}$ и $\Omega^n(A) \setminus \mathfrak{M}$ перечислимы. Дадим набросок разрешающей процедуры для $\mathfrak{M}$. Если $\mathfrak{w} \in \Omega^n(A)$, то применим к $\mathfrak{w}$ поэтапно и поочередно разрешающие процедуры для $\mathfrak{M}$ и $\Omega^n(A) \setminus \mathfrak{M}$ (мы пере-

[1]) См. также МТВФ I, п. 6 § 1.—*Прим. перев.*

межаем шаги одной процедуры шагами другой). Если выполнение одной из них становится невозможным, продолжаем выполнять оставшуюся, которая в этом случае обязательно выполнима, так как обе процедуры за конечное число шагов дают только конечное число элементов. Сравниваем с $\mathfrak{w}$ каждый элемент, получаемый таким способом. При первом совпадении (это когда-нибудь непременно произойдет) прекращаем все действия. Если $\mathfrak{w}$ получено перечислительной процедурой для $\mathfrak{M}$, то $\mathfrak{w} \in \mathfrak{M}$, если нет, то $\mathfrak{w} \in \Omega^n(A) \setminus \mathfrak{M}$.

§ 3. *Перечислимость по Тьюрингу*

В дальнейшем A есть некоторый фиксированный алфавит, $n \geqslant 1$ и $\mathfrak{M} \subset \Omega^n(A)$.

1. Определение и описание перечислимых по Тьюрингу множеств

В соответствии с 2.2 мы даем следующее

3.1. Определение. Множество $\mathfrak{M}$ называется *перечислимым по Тьюрингу* (короче, п. Т.) в том и только в том случае, когда существуют алфавит E и в. Т. функции $f_1, \ldots, f_n$ из $\Omega(E)$ в $\Omega(A)$, такие, что

$$\mathfrak{M} = \left\{ (f_1(w), \ldots, f_n(w)) : w \in \bigcap_{i=1}^{n} \operatorname{Def} f_i \right\}.$$

Квантор существования в 3.1, как и в 1.1, следует понимать в классическом смысле.

Пусть $\mathfrak{M}$ есть п. Т. множество и

$$\mathfrak{M} = \left\{ (f_1(w), \ldots, f_n(w)) : w \in \bigcap_{i=1}^{n} \operatorname{Def} f_i \right\}$$

есть представление $\mathfrak{M}$ в смысле 3.1. Пусть $\sigma_n, \sigma_{n1}, \ldots, \sigma_{nn}$ суть в. Т n-членные функции над $\Omega(A \cup E)$ (ср. МТВФ II, п. 9 § 3). Для всех $i \in \{1, \ldots, n\}$ и $w \in \Omega(E)$ мы определим $h_i(w) \cong \sigma_{ni}(\sigma_n(f_1(w), \ldots, f_n(w)))$ [1]. Согласно МТВФ II, п. 6 § 4, функции h_i являются в. Т. функ-

[1]) По поводу знака $\cong$ см. примечание на стр. 67.

циями из $\Omega(E)$ в $\Omega(A)$ с общей областью определения $\mathfrak{D}=\bigcap_{i=1}^{n}\mathrm{Def}\, f_i$. Ввиду того что $f_i(w)=h_i(w)$, когда $w\in\mathfrak{D}$, имеем

$$\mathfrak{M}=\{(h_1(w), \ldots, h_n(w)) : w\in\mathfrak{D}\}.$$

Далее, если E' — произвольный алфавит и γ — взаимно однозначное в. Т. отображение $\Omega(E')$ на $\Omega(E)$ (ср. МТВФ II, п. 9 § 3), то

$$\mathfrak{M}=\{(h_1(\gamma(w)), \ldots, h_n(\gamma(w))) : w\in\gamma^{-1}(\mathfrak{D})\}$$

есть представление множества $\mathfrak{M}$ в смысле 3.1 с алфавитом E' вместо E и в. Т. функциями $h_1\circ\gamma, \ldots, h_n\circ\gamma$ из $\Omega(E')$ в $\Omega(A)$ с общей областью определения $\gamma^{-1}(\mathfrak{D})$. Таким образом, мы получили следующую теорему:

3.2. Теорема. *Пусть E — произвольный алфавит. Множество $\mathfrak{M}$ является п. Т. множеством тогда и только тогда, когда существуют в. Т. функции $f_1, \ldots, f_n$ из $\Omega(E)$ в $\Omega(A)$ с общей областью определения $\mathfrak{D}$, такие, что $\mathfrak{M}=\{(f_1(w), \ldots, f_n(w)) : w\in\mathfrak{D}\}$.*

(Можно было бы потребовать уже в 3.1, чтобы функции f_i имели общую область определения. Мы воздержались от этого, чтобы дать такое определение, которое гарантировало бы, что *n произвольных* в. Т. функций из $\Omega(E)$ в $\Omega(A)$ определяют, согласно представлению 3.1, некоторое п. Т. подмножество $\Omega''(A)$. Рассмотренные в МВТФ II примеры в. Т. функций доставляют нам тем самым целый набор примеров п. Т. множеств.)

Следующая теорема дает нам полезное в техническом отношении описание п. Т. множеств:

3.3. Теорема. *Множество $\mathfrak{M}$ является п. Т. множеством тогда и только тогда, когда $\mathfrak{M}$ есть область определения некоторой в. Т. функции из $\Omega^n(A)$.*

Мы начнем доказательство с проведения редукции к случаю $n=1$ [1]). Обозначим для этого знаком § первый не входящий в число букв алфавита A символ в после-

[1]) Имея в виду 4.8 и § 5, мы осуществим эту редукцию, не используя σ-функции из МТВФ II, п. 9 § 3.

довательности $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ... и через φ — отображение $\Omega^n(A)$ в $\Omega(A \cup \{\S\})$, для которого $\varphi(w_1, \ldots, w_n) = w_1\S\, w_2\S \ldots \S w_n$ ($w_1, \ldots, w_n \in \Omega(A)$); φ является в. Т. функцией. Мы утверждаем следующее:

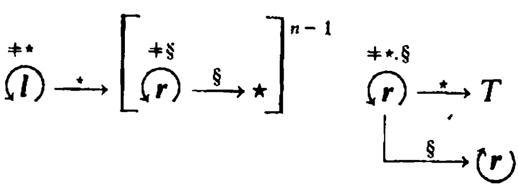
3.4. (a) Множество $\mathfrak{M}$ является п. Т. множеством тогда и только тогда, когда $\varphi(\mathfrak{M})$ есть п. Т. множество.

(b) $\mathfrak{M}$ является областью определения некоторой в. Т. функции из $\Omega^n(A)$ тогда и только тогда, когда $\varphi(\mathfrak{M})$ есть область определения некоторой в. Т. функции из $\Omega(A \cup \{\S\})$.

Доказательство. (a) Предположим сначала, что $\mathfrak{M}$ есть п. Т. множество и $\mathfrak{M} = \{(f_1(w), \ldots, f_n(w)) : w \in \mathfrak{D}\}$ есть некоторое представление $\mathfrak{M}$ в смысле 3.2, где $E = A$. Функция h из $\Omega(A)$ в $\Omega(A \cup \{\S\})$, для которой $\mathrm{Def}\, h = \mathfrak{D}$ и $h(w) = \varphi(f_1(w), \ldots, f_n(w))$, является в. Т. функцией и при этом $\varphi(\mathfrak{M}) = \{h(w) : w \in \mathfrak{D}\}$. Итак, $\varphi(\mathfrak{M})$ есть п. Т. множество.

Обратно, пусть $\varphi(\mathfrak{M})$ есть п. Т. множество и $\varphi(\mathfrak{M}) = \{h(w) : w \in \mathfrak{D}\}$ — некоторое представление $\varphi(\mathfrak{M})$ в смысле 3.2, где $E = A$ и $n = 1$. Функции $g_1, \ldots, g_n$ из $\Omega(A \cup \{\S\})$ в $\Omega(A)$, определяемые соотношениями $\mathrm{Def}\, g_i = \varphi(\Omega^n(A))$ и $g_i(w_1\S \ldots \S\, w_n) = w_i$ для всех $w_1, \ldots, w_n \in \Omega(A)$, являются в. Т. функциями, а поэтому такими будут также и функции $f_1, \ldots, f_n$ из $\Omega(A)$ в $\Omega(A)$, для которых $\mathrm{Def}\, f_i = \mathfrak{D}$ и $f_i(w) = g_i(h(w))$ при всех $w \in \mathfrak{D}$. Следовательно, и $\mathfrak{M} = \{(f_1(w), \ldots, f_n(w)) : w \in \mathfrak{D}\}$ будет п. Т. множеством.

(b) Предположим, не ограничивая общности, что $n \geqslant 2$ и f есть в. Т. функция из $\Omega^n(A)$ в $\Omega(B)$, причем $\mathrm{Def}\, f = \mathfrak{M}$. Пусть м. Т. T вычисляет функцию f. Рассмотрим машину T', описываемую следующей диаграммой:



Вычисляемая машиной T' в. Т. функция f' из $\Omega(A \cup \{\S\})$ в $\Omega(B)$ не определена для аргументов, не принадлежащих $\varphi(\Omega^n(A))$. Это является результатом работы той части машины T', которая не содержит T и которая переводит все допустимые аргументы в их n-членные прообразы относительно отображения φ. Из этого следует, что $\mathrm{Def}\, f' = \varphi(\mathfrak{M})$, что и требовалось доказать.

Обратное утверждение доказывается аналогично, и мы опустим его проверку.

Пользуясь 3.4, мы можем в доказательстве теоремы 3.3 ограничиться случаем $n = 1$. Мы докажем сначала более простую часть теоремы: импликацию справа налево.

Допустим, что $\mathfrak{M}$ есть область определения некоторой в. Т. функции f из $\Omega(A)$ и T — некоторая м. Т., *нормированно* вычисляющая f. (По поводу определения нормированного вычисления см. МТВФ I, 2.2.) Тогда диаграмма

$$T\overset{**}{\frown}(l)$$

определяет м. Т. T', действующую следующим образом: после применения к слову $w \in \Omega(A)$ она сначала *нормированно* вычисляет $f(w)$, если $f(w)$ существует, а затем останавливается после w. Следовательно, определяемая машиной T' в. Т. функция f' из $\Omega(A)$ в $\Omega(A)$ удовлетворяет соотношениям

$$\mathrm{Def}\, f' = \mathrm{Def}\, f, \quad f'(w) = w \qquad (w \in \mathrm{Def}\, f'),$$

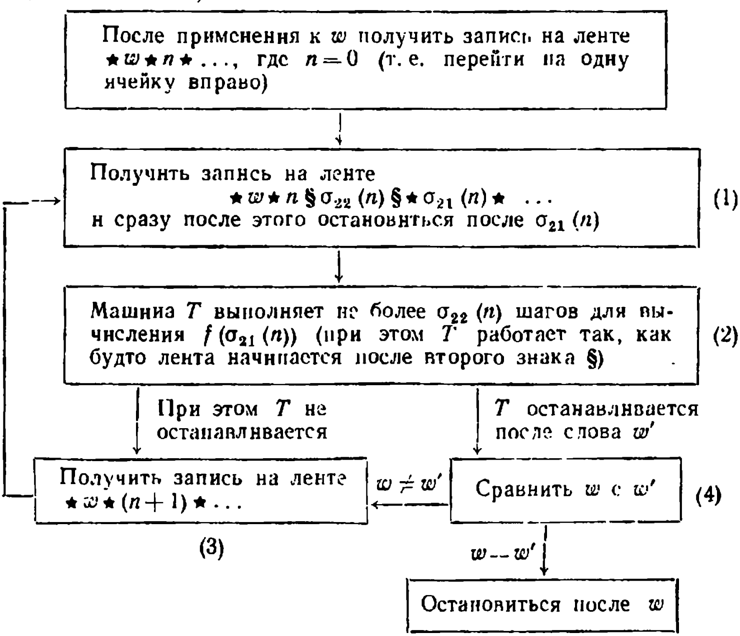
так что
$$\mathfrak{M} = \{f'(w) : w \in \mathrm{Def}\, f'\},$$

т. е. $\mathfrak{M}$ есть п. Т. множество.

Перейдем теперь к доказательству второй части теоремы 3.3. Предположим, что $\mathfrak{M}$ есть п. Т. множество. Очевидно, достаточно доказать существование м. Т. T', которая в результате применения к слову $w \in \Omega(A)$ останавливается после некоторого слова тогда и только тогда, когда $w \in \mathfrak{M}$. Мы не будем приводить здесь доказательство существования во всех деталях, но изложим его достаточно подробно, с тем чтобы его полное восстановление требовало лишь простых технических выкладок.

Ввиду 3.2 мы можем считать, что имеется некоторая в.Т.функция f из $\mathbf{N}$ в $\Omega(A)$, для которой $\mathfrak{M} = \{f(n) : n \in \mathrm{Def}\, f\}$. Пусть T есть некоторая м. Т., *нормированно* вычисляющая функцию f, с рабочим алфавитом A', содержащим A. Мы предложим следующий способ построения T'. Будем исходить из некоторого слова w над A. Включение $w \in \mathfrak{M}$ имеет место в том и только в том случае, когда w есть некоторый f-образ, иными словами, когда существуют n_1 и n_2, такие, что в результате применения к n_1 машина T останавливается после слова w не более чем через n_2 шагов.

Используя пару в. Т. функций σ_{21} и σ_{22} над $\mathbf{N}$ (см. МТВФ II, п. 9 § 3), мы выразим это же несколько иначе: найдется такое n, что в результате применения к $\sigma_{21}(n)$ машина T останавливается после слова w не более чем через $\sigma_{22}(n)$ шагов. Таким образом, доказательство будет закончено, если мы сможем указать м. Т. T', которая после применения к w вычисляет $f(\sigma_{21}(n))$ в соответствии с порядком работы машины T, выполняя последовательность шагов $n=0, 1, \ldots$ вплоть до $\sigma_{22}(n)$-го шага, и останавливается в том и только в том случае, когда результат станет впервые равен w. Машина T может быть описана следующей блок-схемой (где через § обозначена первая буква в последовательности символов $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$, не принадлежащая A'):



Поясним эту схему. Для выполнения (1) необходимы две м. Т., нормированно вычисляющие σ_{21}, соотв. σ_{22}. Часть (2) может быть реализована с помощью следующего машинного фрагмента: составим диаграмму T, пользуясь для этого только элементарными машинами $\boldsymbol{r}$, $\boldsymbol{l}$, $\boldsymbol{a}_i$, а затем каждую стрелку вида $\xrightarrow{a}$ заменим машиной

$$\begin{tikzcd} {} \arrow[r, "a"] & \S\, l \arrow[loop above, "\neq \S"] \arrow[r, "\S"] & l \arrow[loop above, "\neq |, \S"] \arrow[r, "|"] \arrow[d, "\S"] & \star \left[\overset{\neq \S}{\circlearrowleft r} \right]^2 a \arrow[r, "a"] & {} \\ & & {} & & \end{tikzcd}$$

причем направленная вниз стрелка ведет к машинному фрагменту, выполняющему (3), а все в целом связано с машинным фрагментом, реализующим (4). Включением в схему этих машинных фрагментов мы добьемся того, что после каждого шага T будет стираться один штрих $\sigma_{22}(n)$ и T будет работать не долее того момента, когда $\sigma_{22}(n)$ будет стерто. После выполнения (2) запись на ленте будет выглядеть следующим образом:

$$\bigstar\, w \bigstar\, n \,\S\, a_1 \ldots a_{\sigma_{22}(n)} \,\S\, b_1 \ldots b_{\sigma_{22}(n)+\sigma_{21}(n)+2} \bigstar \ldots .$$

Машины же, приспособленные для выполнения (3) и (4), построить уже нетрудно.

С помощью 3.3 мы можем получить еще одно характеристическое свойство п. Т. множеств. Пусть T есть м. Т. с рабочим алфавитом, содержащим A. Мы положим

3.5. $\mathfrak{M}(T, A, n) := \{\mathfrak{w} : \mathfrak{w} \in \Omega^n(A)$ и T останавливается после применения к $\mathfrak{w}\}$.

Мы оставим читателю задачу построения (например, методом, аналогичным использованному при конструировании $T^{\$}$ в МТВФ II, п. 1 § 4) такой м. Т. T' с рабочим алфавитом A', содержащим A, чтобы

$\mathfrak{M}(T, A, n) = \{\mathfrak{w} : \mathfrak{w} \in \Omega^n(A)$ и T', примененная к $\mathfrak{w}$, останавливается после некоторого слова$\}$.

Согласно 3.3, $\mathfrak{M}(T, A, n)$ есть п. Т. множество, так как оно является областью определения порожденной T' в. Т. функции из $\Omega^n(A)$ в $\Omega(A')$.

Если, обратно, $\mathfrak{M}$ есть п. Т. множество, то, согласно 3.3, имеется в. Т. функция f из $\Omega^n(A)$, для которой $\mathrm{Def}\, f = \mathfrak{M}$. Пусть T есть м. Т. с содержащим A рабочим алфавитом, *нормированно* вычисляющая f. Тогда $\mathrm{Def}\, f = \mathfrak{M}(T, A, n)$, так что $\mathfrak{M} = \mathfrak{M}(T, A, n)$. Этим доказана

3.6. Теорема. *$\mathfrak{M}$ есть п. Т. множество тогда и только тогда, когда имеется м. Т. T с рабочим алфавитом, содержащим A, такая, что $\mathfrak{M} = \mathfrak{M}(T, A, n)$.*

2. Свойства замкнутости перечислимых по Тьюрингу множеств

Ряд теоретико-множественных операций ведет от п. Т. множеств снова к п. Т. множествам. Мы упоминаем о наиболее важных из этих операций в 3.7 и 3.8.

3.7. Теорема. *Если множества $\mathfrak{M}_1, \mathfrak{M}_2 \subset \Omega^n(A)$ перечислимы по Тьюрингу, то $\mathfrak{M}_1 \cap \mathfrak{M}_2$ и $\mathfrak{M}_1 \cup \mathfrak{M}_2$ — также п. Т. множества.*

3.8. Теорема. *Если $n \geqslant 2$ и $\mathfrak{M}$ есть п. Т. множество, п. Т. множествами будут также*

(a) $\{(w_{\pi(1)}, \ldots, w_{\pi(n)}) : (w_1, \ldots, w_n) \in \mathfrak{M}\}$ *для каждой перестановки π набора $\{1, \ldots, n\}$;*

(b) $\{(w_1, \ldots, w_{n-1})$: *существует w_n, для которого $(w_1, \ldots, w_n) \in \mathfrak{M}\}$;*

(c) $\{(w_1, \ldots, w_{n-1}) : (w_1, \ldots, w_{n-1}, w_{n-1}) \in \mathfrak{M}\}$.

Докажем сначала 3.8. Пусть выполнены предположения 3.8. Если для представления $\mathfrak{M}$ в смысле 3.2 используются функции $f_1, \ldots, f_n$, то для представления множеств, описанных в (a) и (b), можно использовать наборы функций $f_{\pi(1)}, \ldots, f_{\pi(n)}$, соотв. $f_1, \ldots, f_{n-1}$. Осталось доказать (c).

Так как $\mathfrak{M}$ есть п. Т. множество, то по 3.6 существует м. Т. T с рабочим алфавитом, содержащим A, такая, что $\mathfrak{M} = \mathfrak{M}(T, A, n)$. Пусть K есть копирующая машина над A (ср. МТВФ II, п. 2 § 3) и T' — м. Т., описываемая диаграммой KT. После применения к $(w_1, \ldots, w_{n-1}) \in \Omega^{n-1}(A)$ машина T' сначала копирует w_{n-1}. Затем начинает работать T. Машина T (а поэтому и T') останавливается в том и только в том случае, если $(w_1, \ldots, w_{n-1}, w_{n-1}) \in \mathfrak{M}$. Тем самым

$$\{(w_1, \ldots, w_{n-1}) : (w_1, \ldots, w_{n-1}, w_{n-1}) \in \mathfrak{M}\} = \mathfrak{M}(T', A, n-1).$$

Ввиду 3.6 получаем (c).

К доказательству 3.7. Пусть выполнены предположения 3.7. Так же как и в доказательстве 3.3, мы можем ввиду 3.4 (a) ограничиться случаем $n=1$. Итак, пусть $n=1$. Согласно 3.3, существуют в. Т. функции f_i из $\Omega(A)$ в $\Omega(B_i)$, для которых $\mathrm{Def}\, f_i = \mathfrak{M}_i$ $(i=1, 2)$. Пусть $B:=B_1 \cup B_2$ и σ_2 есть в. Т. функция двух переменных над B (ср. МТВФ II, п. 9 § 3). Функция h из $\Omega(A)$ в $\Omega(B)$, определенная равенством $h(w) \cong \sigma_2(f_1(w), f_2(w))$ $(w \in \Omega(A))$, является в. Т. функцией и $\mathrm{Def}\, h = \mathfrak{M}_1 \cap \mathfrak{M}_2$. Согласно 3.3, отсюда следует, что $\mathfrak{M}_1 \cap \mathfrak{M}_2$ есть п. Т. множество.

Теперь рассмотрим $\mathfrak{M}_1 \cup \mathfrak{M}_2$. Согласно 3.2, мы можем предполагать, что $\mathfrak{M}_i$ при $i=1, 2$ является образом некоторой в. Т. функции f_i из $\mathbf{N}$ в $\Omega(A)$. Мы рассмотрим функцию g из $\Omega(\{\boldsymbol{a}_1, \boldsymbol{a}_2\})$ в $\Omega(A)$, которая задается следующей процедурой: исходя из слова w над $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$ длины l, вычисляем $f_1(l)$, если $l=0$ или w оканчивается на $\boldsymbol{a}_1$, и $f_2(l-1)$, если $l \geqslant 1$ и w оканчивается на $\boldsymbol{a}_2$. Тогда $\mathrm{Bild}\, g = \mathrm{Bild}\, f_1 \cup \mathrm{Bild}\, f_2$, так что $\mathfrak{M}_1 \cup \mathfrak{M}_2 = \{g(w) : w \in \mathrm{Def}\, g\}$. Нетрудно построить м. Т., вычисляющую g, откуда и будет следовать перечислимость по Тьюрингу множества $\mathfrak{M}_1 \cup \mathfrak{M}_2$.

Стоит отметить, что операция взятия дополнения (относительно $\Omega^n(A)$), вообще говоря, выводит из области п. Т. множеств. В п. 4 мы приведем интересный пример этого явления. То же произойдет, если в 3.8 (b) заменить «существует» на «для всех». Следующее простое рассуждение показывает, что это довольно естественно: если $(w_1, \ldots, w_{n-1})$ задано, то за конечное число шагов можно установить принадлежность $(w_1, \ldots, w_{n-1}, w) \in \mathfrak{M}$, вообще говоря, только для не более чем конечного числа w (а значит, когда $\mathfrak{M}$ бесконечно, не для всех $w \in \mathfrak{M}$).

3. Теорема о перечислимости

В статье МТВФ III, п. 2 § 6, мы установили существование универсальных в. Т. функций. Мы воспользуемся теперь этими функциями, для того чтобы установить существование п. Т. множеств с похожими свойствами универсальности. Точнее, будет доказана

3.9. Теорема. *Существует такое п. Т. подмножество* $\mathfrak{W} \subset \Omega^{n+1}(A)$, *что множества* $\mathfrak{M}_w := \{(w_1, \ldots, w_n): (w, w_1, \ldots, w_n) \in \mathfrak{W}\}$ *пробегают в точности п. Т. подмножества* $\Omega^n(A)$, *когда* w *пробегает* $\Omega(A)$.

Теорема 3.9 известна как одна из форм теоремы Клини о перечислимости (ср. Клини [10]). Она позволяет представлять п. Т. подмножества $\Omega^n(A)$ как «сечения» относительно первой компоненты фиксированного п. Т. подмножества из $\Omega^{n+1}(A)$. Если $\mathfrak{M} = \mathfrak{M}_w$, то w называют *индексом* $\mathfrak{M}$ (относительно $\mathfrak{W}$). Каждое п. Т. подмножество из $\Omega^n(A)$ обладает бесконечным множеством индексов. Индексы играют значительную роль в теории перечислимых множеств. Так как п. Т. множества полностью описываются своими индексами и так как индексы являются конструктивными элементами, то и п. Т. множества становятся благодаря индексации конструктивными элементами и тем самым — допустимыми в качестве аргументов вычислимых функций или в качестве элементов перечислимых множеств.

Как пример использования п. Т. множеств в таком качестве можно упомянуть следующее уточнение теоремы 3.7:

3.7*. *Существуют в. Т. функции* $f_\cap$ *и* $f_\cup$, *отображающие* $\Omega^2(A)$ *в* $\Omega(A)$ *и такие, что для всех* $w_1, w_2 \in \Omega(A)$

$$\mathfrak{M}_{w_1} \cap \mathfrak{M}_{w_2} = \mathfrak{M}_{f_\cap(w_1, w_2)} \quad \text{и} \quad \mathfrak{M}_{w_1} \cup \mathfrak{M}_{w_2} = \mathfrak{M}_{f_\cup(w_1, w_2)}.$$

Более подробные сведения можно найти в книге Роджерса [14].

К доказательству 3.9. Пусть F есть $(n+1)$-местная универсальная функция над алфавитом A из МТВФ III, 6.4. Положим $\mathfrak{W} := \mathrm{Def}\, f$. Согласно 3.3, $\mathfrak{W}$ является п. Т. множеством. Если $w \in \Omega(A)$, то f_w есть в. Т. функция. Так как $\mathrm{Def}\, f_w = \mathfrak{M}_w$, то опять, согласно 3.3, $\mathfrak{M}_w$ есть п. Т. множество. Предположим теперь, что $\mathfrak{M}$ есть п. Т. подмножество $\Omega^n(A)$. Согласно 3.3, $\mathfrak{M}$ является областью определения в. Т. функции f из $\Omega^n(A)$. Как видно из блок-схемы, использованной при доказательстве теоремы 3.3 (стр. 99), f можно выбрать даже таким образом, чтобы она совпадала на Def f с тождественным отображением н, в частности, была функцией из $\Omega^n(A)$ в $\Omega(A)$. Тогда существует $w \in \Omega(A)$, для которого $f = f_w$ и тем самым $\mathfrak{M} = \mathrm{Def}\, f_w = \mathfrak{M}_w$, что и требовалось доказать.

Согласно заключительному замечанию в МТВФ III, 6.4, мы можем эффективно задать м. Т. T, которая *нормированно* вычисляет используемую в доказательстве функцию F. Так как к тому же $\mathfrak{W} = \mathrm{Def}\, F = \mathfrak{M}(T, A, n+1)$, то это замечание переносится на 3.9 в том смысле, что мы можем эффективно задать м. Т. T с $\mathfrak{W} = \mathfrak{M}(T, A, n+1)$.

4. Не перечислимые по Тьюрингу множества

Легко убедиться в существовании не перечислимых по Тьюрингу множеств. Так как, например, $\mathbf{N}$ содержит только счетную совокупность п. Т. подмножеств, а именно (при $A = \{|\}$ и $n = 1$) множества $\mathfrak{M}_m$ с $m \in \mathbf{N}$, то «почти все» подмножества $\mathbf{N}$ не являются п. Т. подмножествами.

Мы укажем теперь два интересных примера. Рассмотрим 3.9 для случая $n = 1$ и положим ($\mathfrak{W}$ фиксировано раз и навсегда [1]))

$$\mathfrak{M}_{\mathrm{Dia}} := \{w : (w, w) \notin \mathfrak{W}\}.$$

(Индекс Dia должен напоминать о «диагонализации».) Тогда имеет место

3.10. Теорема. *Множество* $\mathfrak{M}_{\mathrm{Dia}}$ *не перечислимо по Тьюрингу*; $\Omega(A) \setminus \mathfrak{M}_{\mathrm{Dia}}$ *есть п. Т. множество.*

Доказательство. $\Omega(A) \setminus \mathfrak{M}_{\mathrm{Dia}} = \{w : (w, w) \in \mathfrak{W}\}$ является п. Т. множеством согласно 3.8 (c). Докажем от противного, что $\mathfrak{M}_{\mathrm{Dia}}$ не есть п. Т. множество. Если бы $\mathfrak{M}_{\mathrm{Dia}}$ было п. Т., то по 3.9 существовало бы такое $w_0 \in \Omega(A)$, что $\mathfrak{M}_{\mathrm{Dia}} = \mathfrak{M}_{w_0}$. Отсюда следует, что $w_0 \in \mathfrak{M}_{\mathrm{Dia}}$ тогда и только тогда, когда $w_0 \in \mathfrak{M}_{w_0}$, а это означает, что $(w_0, w_0) \notin \mathfrak{W}$ тогда и только тогда, когда $(w_0, w_0) \in \mathfrak{W}$. Тем самым получено противоречие.

Этим доказано 3.10. Конструкция $\mathfrak{M}_{\mathrm{Dia}}$ напоминает построение $\{x : x$ — множество и $x \notin x\}$, лежащее в основе *антиномии Рассела*. В обеих конструкциях используется

[1]) $\mathfrak{W}$ есть универсальное множество теоремы 3.9. — *Прим. перев.*

процедура диагонализации, восходящая в конечном счете еще к Кантору (доказательство несчетности множества действительных чисел). Подобно тому как конструкция Рассела выводит за пределы царства множеств, так и конструкция $\mathfrak{M}_{\mathrm{Dia}}$ выводит за пределы царства п. Т. множеств. Подробный разбор этой аналогии есть у Роджерса [14], стр. 185.

В качестве следствия 3.10 при $n=1$ получается

3.11. Теорема. *Множество* $\Omega^2(A)\setminus\mathfrak{W}$ *не перечислимо по Тьюрингу.*

Если бы $\Omega^2\setminus\mathfrak{W}$ было п. Т. множеством, то по 3.8 (с) п. Т. множеством было бы и $\{w:(w,w)\in\Omega^2(A)\setminus\mathfrak{W}\}$, т. е. $\mathfrak{M}_{\mathrm{Dia}}$.

(3.10 и 3.11 могут быть перенесены на случай $n>1$. Для этого определяем $\mathfrak{M}_{\mathrm{Dia}}:=\{(w, w_2, \ldots, w_n): (w, w, w_2, \ldots, w_n)\notin\mathfrak{W}\}$ и замечаем, что ввиду 3.8 (а) и 3.8 (с) имеет место аналог 3.8 (с) и для «диагонализации» по первой переменной.)

Теоремы 3.10 и 3.11 дают *приблизительное* представление о так называемой *теореме Гёделя о неполноте* (ср. Гёдель [8]), принадлежащей к важнейшим теоремам метаматематики. Теорема о неполноте утверждает, что при известных требованиях к языку, в котором имеется отрицание, и для логической системы, приспособленной для формального доказательства определенных высказываний в этом языке, справедливо утверждение: существует такое высказывание, что ни оно само, ни его отрицание не могут быть формально доказаны.

В качестве языка мы выберем множество последовательностей знаков («высказываний») $(w_1, w_2)\in\mathfrak{W}$ и $(w_1, w_2)\notin\mathfrak{W}$, где $(w_1, w_2)\in\Omega^2(A)$. Высказывание $(w_1, w_2)\notin\mathfrak{W}$ называется *отрицанием* высказывания $(w_1, w_2)\in\mathfrak{W}$, и наоборот. Мы мотивируем эти обозначения следующим образом: $(w_1, w_2)\in\mathfrak{W}$ истинно, когда $(w_1, w_2)\in\mathfrak{W}$, и ложно в противном случае; $(w_1, w_2)\notin\mathfrak{W}$ истинно, если $(w_1, w_2)\notin\mathfrak{W}$, и ложно в противном случае.

Пусть в рамках этого языка задана логическая система, которая приспособлена для формального доказательства определенных, а точнее, *истинных* высказываний. Мы понимаем под логической системой некоторое *исчис-*

ление (ср. по этому поводу § 4). Из изложенного в двух следующих параграфах вытекает, что объекты, выводимые в некотором исчислении, образуют п.Т. множество. Поэтому в нашем случае на интуитивном уровне довольно легко понять, что

$$\mathfrak{W}^+ := \{(w_1, w_2) : (w_1, w_2) \in \mathfrak{W} \text{ формально доказуемо}\}$$

есть п.Т. подмножество $\mathfrak{W}$ и

$$\mathfrak{W}^- := \{(w_1, w_2) : (w_1, w_2) \notin \mathfrak{W} \text{ формально доказуемо}\}$$

есть п.Т. подмножество $\Omega^2(A) \setminus \mathfrak{W}$. Согласно 3.11, $\mathfrak{W}^-$ является *собственным* подмножеством $\Omega^2(A) \setminus \mathfrak{W}$, так что $\mathfrak{W}^+ \cup \mathfrak{W}^-$ является *собственным* подмножеством $\Omega^2(A)$. Тем самым доказано существование элемента $(w_1, w_2) \in \Omega^2(A)$, не принадлежащего ни $\mathfrak{W}^+$, ни $\mathfrak{W}^-$, для которого в вышеописанной логической системе не может быть формально доказано ни $(w_1, w_2) \in \mathfrak{W}$, ни $(w_1, w_2) \notin \mathfrak{W}$. Таким элементом будет, например, (w_0, w_0), если w_0 есть индекс множества $\{w : (w, w) \in \mathfrak{W}^-\}$, так как в этом случае имеет место предложение: $(w_0, w_0) \in \mathfrak{W}^-$ тогда и только тогда, когда $(w_0, w_0) \in \mathfrak{W}$. Ввиду того что $\mathfrak{W}^- \cap \mathfrak{W}$ пусто, эта эквивалентность имеет место только тогда, когда $(w_0, w_0) \notin \mathfrak{W}^- \cup \mathfrak{W}$ и, в частности, когда $(w_0, w_0) \notin \mathfrak{W}^- \cup \mathfrak{W}^+$.

Мы закончим обсуждение п.Т. множеств одним следствием из вышеизложенных рассуждений, которое потребуется нам в § 5 для того, чтобы, как уже говорилось в введении, обратиться к другому уточнению понятия перечислимости, так называемой *перечислимости по Шмульяну*.

Согласно заключительному замечанию к доказательству 3.9, можно эффективно задать м.Т. T с рабочим алфавитом, содержащим A, которая нормированно вычисляет F, причем так, чтобы множество $\mathfrak{W} = \mathrm{Def}\, F = \mathfrak{M}(T, A, n+1)$ удовлетворяло 3.9. Пусть теперь снова $n = 1$, и пусть K есть копирующая машина для A, а T' есть м.Т., задаваемая диаграммой KT. Поскольку $\Omega(A) \setminus \mathfrak{M}_{\mathrm{Dia}} = \{w : (w, w) \in \mathfrak{W}\}$, то $\Omega(A) \setminus \mathfrak{M}_{\mathrm{Dia}} = \mathfrak{M}(T', A, 1)$, как, в частности, было уже показано в доказательстве 3.8 (c). По 3.10 $\mathfrak{M}_{\mathrm{Dia}}$ не является п.Т. множеством. Нами получена

3.12. Теорема. *Можно эффективно задать м.Т. T' с рабочим алфавитом, содержащим A, такую, что $\Omega(A) \setminus \mathfrak{M}(T', A, 1)$ не является п.Т. множеством, причем T' нормированно вычисляет определяемую ею функцию, отображающую $\Omega(A)$ в $\Omega(A)$.*

(Согласно 2.3, для такой машины, наглядно говоря, неразрешимо, останавливается ли она после применения к некоторому слову над A через конечное число шагов, или нет (ср. МТВФ II, п. 2 § 5).)

§ 4. Перечислимость по Шмульяну

1. Построение множеств с помощью исчислений

При разъяснении понятия перечислимости по Тьюрингу мы существенно использовали тот факт, что для каждого перечислимого множества существует однозначно выполнимая перечислительная процедура. Теперь мы попытаемся дать набросок предписания для перечислительной процедуры, не удовлетворяющей требованию однозначной выполнимости. (Для простоты мы ограничимся множествами слов[1].)

Такое предписание должно позволять выписывать определенные (в предельном случае—никакие) слова и *порождать* новые; возможно, что оно содержит также указания, устанавливающие, как и когда можно порождать новые слова, исходя из уже полученных слов. Кроме того, не каждое порожденное слово обязано принадлежать перечислимому множеству,—предписание может содержать так называемое *правило выбора*, с помощью которого можно будет решить, принадлежит ли порожденное слово нашему множеству или нет.

Конечную совокупность вышеописанных указаний (без правила выбора) мы называем *исчислением*, сами указания—*правилами* исчисления. Те правила, которые позволяют получать слова без использования ранее полученных слов, можно представлять себе как правила, согласно

[1] То есть пока рассматривается частный случай n-последовательностей слов, где $n=1$.— *Прим. перев.*

которым можно порождать новые слова, исходя из пустого множества порожденных слов.

Слово называется *порождаемым* или *выводимым в исчислении*, если оно может быть получено согласио правилам нсчисления. Под *выводом относительно исчисления* мы понимаем конечную не пустую последовательность слов, обладающую тем свойством, что каждый член последовательности может быть получен из некоторого набора предшествующих членов согласно правилам исчисления. Очевидно, что слово тогда и только тогда выводимо в некотором исчислении, когда существует вывод относительно этого исчисления, оканчивающийся этим словом.

В этой новой и пока еще интуитивно-наглядной терминологии определение 1.1 для множеств слов может быть теперь сформулировано следующим образом:

4.1. Множество $\mathfrak{M}$ слов перечислимо тогда и только тогда, когда существуют такое исчисление и такое правило выбора, что все выводимые в этом исчислении слова, удовлетворяющне правилу выбора, и только они принадлежат $\mathfrak{M}$.

Мы воздержимся от более подробного анализа интуитивного понятия исчисления, так как такой анализ, повидимому, был бы в значительной степени анализом интуитивного понятия алгоритма. (Сошлемся, однако, на превосходное изложение этой темы у Лоренцена [11].) Вместо этого мы на одном примере уточним это пока еще очень расплывчатое описание исчислений, а в следующих пунктах дадим точное определение одного класса исчислений, так называемых *формальных систем Шмульяна*, которые будут лежать в основе наших дальнейших рассмотрений.

Пример исчисления. Будем исходить из алфавита $A=\{a_1, a_2, a_3\}$. Вместо букв a_1, a_2, a_3 соответственно будем использовать имеющие наглядный смысл символы $|$, $\times$, $=$.

Правило 1. Можно напнсать слово $\times=$.

Правило 2. Если написано слово $w\times w'=w''$, то можно написать слово $w\times w'|=w''w$.

Правило 3. Если написано слово $w\times w' = w''$, то можно написать слово $w|\times w' = w''w'$.

Правило 4. Если написано слово $w\times w = w'$, то можно написать слово w'.

Пользуясь первыми тремя правилами, можно писать слова вида $w\times w' = w''$, где w, w', $w''\in \mathrm{N}$ и $w\cdot w' = w''$, и только эти слова (точка обозначает умножение в N). Легко показать индукцией (по длине слова), что мы получим таким образом все слова этого вида. (Заметим, что мы отождествляем 0 и $\square$.) Обратное утверждение доказывается индукцией по длине вывода $\mathfrak{A}$ для $w\times w' = w''$. Если $\mathfrak{A}$ имеет длину 1, то $w\times w' = w''$ получается обязательно по первому правилу, так что $w = w' = w'' = \square$, и тем самым $w, w', w''\in \mathrm{N}$ и $w\cdot w' = w''$. Пусть $\mathfrak{A}$ имеет длину >1 — это индуктивное предположение. Если $w\times w' = w''$ получается с помощью первого правила, то рассуждаем так же, как на начальном шаге индукции. Если в качестве последнего правила в $\mathfrak{A}$ используется, например, второе правило (для третьего правила все проходит аналогично), то в $\mathfrak{A}$ имеется член вида $\bar w\times \bar w' = \bar w''$, так что $w\times w' = w'' = \bar w\times \bar w'| = \bar w''\bar w$. Применив индуктивное предположение к слову $\bar w\times \bar w' = \bar w''$ (обладающему более коротким выводом, чем $\mathfrak{A}$), получим $\bar w$, $\bar w'$, $\bar w''\in \mathrm{N}$ и $\bar w\cdot \bar w' = \bar w''$. Отсюда следует, что $\bar w = w$, $\bar w'| = w'$ и $\bar w''\bar w = w''$, поэтому w, w', $w''\in \mathrm{N}$ и $w\cdot w' = w''$.

Подобным же образом можно показать, что все слова над A, получаемые согласно четвертому правилу, и только они являются квадратами. В качестве примера рассмотрим здесь вывод для $||||$ с понятными комментариями:

$\times =$	(правило 1),
$\times | =$	(правило 2 к $\times =$),
$\times || =$	(правило 2 к $\times | =$),
$|\times || = ||$	(правило 3 к $\times || =$),
$||\times || = ||||$	(правило 3 к $|\times || = ||$),
$||||$	(правило 4 к $||\times || = ||||$).

Если правило выбора исключает из рассмотрения те и только те порожденные исчислением слова, которые содержат символ $\times$ (или $=$), то мы получим доказательство того факта, что множество полных квадратов перечислимо.

2. Формальные системы Шмульяна

Наряду с до сих пор использовавшимися алфавитами, в основу которых была положена последовательность символов a_1, a_2, ..., мы введем два новых типа алфавитов. Мы будем исходить из двух новых последовательностей символов v_1, v_2, ... и p_1, p_2, ..., отличных как от a_i, так и друг от друга. Символы v_i мы будем называть *переменными*, а p_i — *предикатами*. В качестве обозначений для переменных мы используем буквы v, ..., для предикатов — буквы p, ... Алфавит, образованный членами непустого начального отрезка конечной длины последовательности переменных, мы называем *алфавитом переменных*. Аналогично определяется *алфавит предикатов*. Пусть, наконец, $\rightarrow$ и ; суть два новых символа.

Для определения формальной системы Шмульяна нам необходимы некоторые приготовления.

4.2. Определение. Формальный базис Φ есть четверка (A, V, P, S), состоящая из алфавита A, алфавита переменных V, алфавита предикатов P и последовательности S натуральных чисел, длина которой равняется числу элементов P. Если $p_i \in P$, то i-й член S (обозначаемый в дальнейшем S_i) называется Φ-*порядком* p_i[1]). Элементы множества $\Omega(A)$ называются Φ-*словами*, а элементы $\Omega(A \cup V)$ называются Φ-*термами*.

В качестве обозначений для Φ-слов и Φ-термов используются буквы w, ..., соотв. t, ... Примерами Φ-слов являются (для любого Φ), например, $\square$ и a_1a_1; Φ-термами будут, например, $\square$, a_1a_1, v_1 и $a_1v_1v_1$.

Теперь мы индуктивно определим (атомарные) Φ-*формулы*.

4.3. Определение. Пусть $\Phi = (A, V, P, S)$ есть формальный базис;

---

[1]) Это означает, что p_i есть S_i-местный предикат.— *Прим. перев.*

(a) *атомарными* Ф-формулами называются последовательности символов $p_i t_1; \ldots; t_{S_i}$ с Ф-термами $t_1, \ldots, t_{S_i}$ и $p_i \in P$ и только они;

(b) *Ф-формулы* — это *атомарные* Ф-формулы и последовательности символов вида $\alpha \to \beta$, где α и β суть Ф-формулы, и только они.

Если Ф-порядок p_1 есть 2, то атомарной формулой будет, например, $p_1\square; a_1v_1$; Ф-формулами будут $p_1\square; a_1v_1$ и $p_1\square; \square \to p_1v_1; a_1 \to p_1a_1; \square$.

Вместо того чтобы определять Ф-формулы *индуктивно*, как в 4.3 (b), их можно получать, используя некоторое исчисление. Мы оставляем читателю построение подходящей системы правил. В качестве обозначений для Ф-формул мы используем буквы α, β, ...

Далее мы вводим понятие подстановки Ф-формул.

4.4. Определение. Пусть Ф — формальный базис и α есть некоторая Ф-формула; *Ф-подстановка* α есть некоторая последовательность знаков, получаемая из α *заменой всех переменных Ф-словами*, причем *одинаковые* переменные заменяются *одинаковыми* Ф-словами.

Ф-подстановка Ф-формулы есть *свободная от переменных* Ф-формула. Например, если $\Phi = (\{a_1, a_1\}, \{v_1, v_2\}, \{p_1, p_2\}, S)$ и $S = 1, 1$, то

$$p_1a_1 \to p_2a_1a_2a_1a_1 \to p_1a_1a_2a_2a_1$$

есть Ф-подстановка Ф-формулы $p_1v_1 \to p_2a_1v_2a_1 \to p_1v_1a_2v_2$ (v_1 заменена на a_1, v_2 — на a_2a_1).

Если Ф-формула не содержит переменных, то она сама является своей единственной Ф-подстановкой.

Нетрудно было бы дать точное определение замены, введя исчисление подстановок. Но мы полагаем, что ввиду наглядности процедуры замены от этого можно отказаться.

Пусть теперь Ф есть формальный базис и П — *конечное* множество Ф-формул. Согласно несколько ослабленному варианту оригинального определения Шмульяна [15], мы сопоставляем паре (Ф, П) некоторое исчисление Σ(Ф, П), состоящее из следующих двух правил:

Правило 1 (правило подстановки). Можно написать произвольную Ф-подстановку произвольной Ф-формулы из П.

Правило 2 (Modus Ponens). Если α — некоторая *атомарная* Φ-формула и выписана Φ-формула $\alpha \to \beta$, то можно написать формулу β; α и $\alpha \to \beta$ называются в этом случае *посылками* конкретного применения правила.

Второе правило напоминает *логическое* правило Modus Ponens, согласно которому от двух высказываний: $\mathfrak{a}$ и *если* $\mathfrak{a}$, *то* $\mathfrak{b}$ можно перейти к высказыванию $\mathfrak{b}$.

Элементы Π называются *заключениями* исчисления $\Sigma(\Phi, \Pi)$; *атомарные* заключения $\Sigma(\Phi, \Pi)$ называются *аксиомами* $\Sigma(\Phi, \Pi)$.

4.5. Определение. Σ является *формальной системой Шмульяна* (сокращенно с. Ш.) тогда и только тогда, когда существуют формальный базис Φ и *конечное* множество Φ-формул Π, такие, что $\Sigma = \Sigma(\Phi, \Pi)$.

Если $\Sigma = \Sigma(\Phi, \Pi)$ есть с.Ш., то чтобы выразить тот факт, что α есть выводимая в Σ Φ-формула, мы будем писать $\Sigma \vdash \alpha$. Первую компоненту A базиса Φ мы будем называть *рабочим алфавитом* системы Σ.

Прежде чем на нескольких примерах пояснить содержание понятия с.Ш., стоит сначала определить, что мы будем понимать под множествами, *перечислимыми по Шмульяну*.

4.6. Определение. Пусть $n \geqslant 1$ и $\mathfrak{M} \subset \Omega^n(A)$. Множество $\mathfrak{M}$ называется *перечислимым по Шмульяну* (сокращенно п.Ш.) множеством тогда и только тогда, когда существует с.Ш. $\Sigma = \Sigma(\Phi, \Pi)$ со следующими свойствами:

(1) Рабочий алфавит Σ содержит A.

(2) Φ-порядок $\boldsymbol{p}_1$ равен n.

(3) Для всех Φ-слов $w_1, \ldots, w_n$ включение $(w_1, \ldots, w_n) \in \mathfrak{M}$ имеет место тогда и только тогда, когда $\Sigma \vdash \boldsymbol{p}_1 w_1; \ldots; w_n$.

Квантор существования следует понимать и здесь, и во всех предыдущих определениях такого рода в *классическом* смысле.

Наглядный смысл этого определения состоит в том, что система Шмульяна, в которой, согласно 4.6, выводимо $\mathfrak{M}$, оперирует с S_i-членными последовательностями слов над рабочим алфавитом, причем эти S_i-членные последовательности в зависимости от предиката, после которого они стоят, будут считаться принадлежащими различным, но не обязательно непересекающимся классам. Принадлежность к классу, выделяемому предикатом p_1, соответствует как раз правилу выбора. Очевидно, тот факт, что мы выделили именно p_1, не играет никакой роли.

Теперь приведем несколько примеров.

4.7(1). Пусть $\Phi := (A, \{v_1\}, \{p_1\}, 1)$,

$$\Pi := \{p_1\} \cup \{p_1v_1 \to p_1v_1a : a \in A\}$$

(здесь $p_1 = p_1\square$),

$$\Sigma := \Sigma(\Phi, \Pi).$$

Покажем сначала, построив соответствующий вывод, что, скажем, $p_1a_1a_1$ выводимо в Σ:

p_1	(Ф-подстановка p_1),
$p_1 \to p_1a_1$	(Ф-подстановка $p_1v_1 \to p_1v_1a_1$),
$p_1a_1 \to p_1a_1a_1$	(Ф-подстановка $p_1v_1 \to p_1v_1a_1$),
p_1a_1	(Modus Ponens в применении к p_1 и $p_1 \to p_1a_1$),
$p_1a_1a_1$	(Modus Ponens в применении к p_1a_1 и $p_1a_1 \to p_1a_1a_1$).

Далее, индукцией по длине слова w покажем, что $\Sigma \vdash p_1w$ для всех Ф-слов w ($\Omega(A)$ также является п.Ш. множеством).

База индукции: p_1 есть вывод относительно Σ, так что $\Sigma \vdash p_1w$ при $w = \square$.

Шаг индукции. Предположим, что w представимо в виде $w'a$ ($a \in A$), и для w' утверждение доказано. Тогда существует вывод относительно Σ, оканчивающийся формулой p_1w'. К этому выводу можно добавить следующие формулы:

$p_1w' \to p_1w'a$	(Ф-подстановка $p_1v_1 \to p_1v_1a$),
$p_1w'a$	(Modus Ponens, примененный к двум последним формулам вывода).

Отсюда следует, что $\Sigma \vdash p_1w$. (Стоит сравнить 4.7 (1) и 1.4 (2)!)

4.7 (2). (В связи с этим см. также пример исчисления на стр. 108.) Пусть

$\Phi := (\{|\}, \{v_1, v_2, v_3\}, \{p_1, p_2\}, S)$, где $S = 1, 3$,

(Для большей наглядности мы будем писать *Квадр* вместо p_1 и *Умнож* вместо p_2.)

П состоит из следующих Ф-формул:

Умнож $\square; \square; \square$ ($\square$ стоит здесь лишь для определенности),

Умнож $v_1; v_2; v_3 \to$ *Умнож* $v_1; v_2 |; v_3 v_1$,

Умнож $v_1; v_2; v_3 \to$ *Умнож* $v_1 |; v_2; v_3 v_2$,

Умнож $v_1; v_1; v_2 \to$ *Квадр* v_2.

$\Sigma := \Sigma(\Phi, \Pi)$.

Как и в примере исчисления на стр. 108, можно показать, что $\Sigma \vdash$ *Квадр* w тогда и только тогда, когда w есть квадрат некоторого числа. Отсюда следует, что квадраты образуют п. Ш. множество.

3. Редукция к множествам слов

Мы не объяснили, почему понятие перечислимости по Шмульяну может рассматриваться наряду с понятием перечислимости по Тьюрингу как адекватное уточнение понятия перечислимости. Прежде чем обратиться к этому вопросу (в § 5), мы хотели бы показать, что в наших рассуждениях можно ограничиться *множествами слов*.

Пусть $n \geqslant 1$, $\mathfrak{M} \subset \Omega^n(A)$ и φ есть использованное в 3.4 отображение $\Omega^n(A)$ в $\Omega(A \cup \{\S\})$. В качестве аналога 3.4 (а) докажем такое утверждение:

4.8. Теорема. *Множество* $\mathfrak{M}$ *перечислимо по Шмульяну тогда и только тогда, когда* $\varphi(\mathfrak{M})$ *есть п. Ш. множество.*

Доказательство. Предположим сначала, что $\varphi(\mathfrak{M})$ есть п. Ш. множество и $\tilde{\Sigma} = \Sigma(\tilde{\Phi}, \tilde{\Pi})$ есть с. Ш., порождающая $\varphi(\mathfrak{M})$. Пусть при этом $\tilde{\Phi} = (\tilde{A}, \{v_1, \ldots, v_k\}, \{p_1, \ldots, p_l\}, \tilde{S})$. Положим

$$\Phi := (\tilde{A}, \{v_1, \ldots, v_{\max(n, k)}\}, \{p_1, \ldots, p_{l+1}\}, S)$$

и $S_1 := n$, $S_i := \tilde{S}_{i-1}$ $\quad (2 \leqslant i \leqslant l+1)$.

Пусть П состоит из Ф-формул, которые получаются из элементов $\tilde{\Pi}$ увеличением индексов всех предикатов на 1, а также из Ф-формул вида $p_2 v_1 \S \ldots \S v_n \to p_1 v_1; \ldots; v_n$.

Определим
$$\Sigma := \Sigma(\Phi, \Pi);$$
Σ порождает $\mathfrak{M}$, так как для слов $w_1, \ldots, w_n$ над $\tilde{A}\,(\supset A)$ следующие высказывания эквивалентны:

(1) $\Sigma \vdash \boldsymbol{p}_1 w_1; \ldots; w_n$;

(2) $\Sigma \vdash \boldsymbol{p}_2 w_1 \S \ldots \S w_n$;

(3) $\tilde{\Sigma} \vdash \boldsymbol{p}_1 w_1 \S \ldots \S w_n$;

(4) $w_1 \S \ldots \S w_n \in \varphi(\mathfrak{M})$;

(5) $(w_1, \ldots, w_n) \in \mathfrak{M}$.

Итак, $\mathfrak{M}$ есть п. Ш. множество.

Заметим между строк, что навыки в обращении с системами Шмульяна полезны при проведении подробных доказательств утверждений, впрочем, достаточно наглядных, которые встречаются как здесь, так и в дальнейшем.

Обратно, пусть $\mathfrak{M}$ есть п. Ш. множество и $\Sigma = \Sigma(\Phi, \Pi)$ есть с. Ш., порождающая $\mathfrak{M}$. Пусть $\Phi = (A', \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}, \{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_l\}, S)$. Мы предположим сначала, что A *строго* содержится в A', причем, в частности, $\S \in A'$. С помощью Σ мы определим с. Ш. $\tilde{\Sigma}$ точно так же, как в первой части доказательства мы определили с помощью $\tilde{\Sigma}$ с. Ш. Σ; при этом в качестве соответствующих следствий из $\tilde{\Pi}$ мы возьмем $\tilde{\Phi}$-формулы
$$\boldsymbol{p}_2 \boldsymbol{v}_1; \ldots; \boldsymbol{v}_n \to \boldsymbol{p}_1 \boldsymbol{v}_1 \S \ldots \S \boldsymbol{v}_n.$$
Тогда для $\tilde{w} \in \Omega(A')$ следующие высказывания эквивалентны:

(1) $\tilde{\Sigma} \vdash \boldsymbol{p}_1 \tilde{w}$.

(2) Существуют $\tilde{w}_1, \ldots, \tilde{w}_n \in \Omega(A')$, для которых
$$\tilde{w}_1 \S \ldots \S \tilde{w}_n = \tilde{w} \text{ и } \tilde{\Sigma} \vdash \boldsymbol{p}_2 \tilde{w}_1; \ldots; \tilde{w}_n.$$

(3) Существуют $\tilde{w}_1, \ldots, \tilde{w}_n \in \Omega(A')$, для которых
$$\tilde{w}_1 \S \ldots \S \tilde{w}_n = \tilde{w} \text{ и } \Sigma \vdash \boldsymbol{p}_1 \tilde{w}_1; \ldots; \tilde{w}_n.$$

(4) Существуют $\tilde{w}_1, \ldots, \tilde{w}_n \in \Omega(A')$, для которых
$$\tilde{w}_1 \S \ldots \S \tilde{w}_n = \tilde{w} \text{ и } (\tilde{w}_1, \ldots, \tilde{w}_n) \in \mathfrak{M}.$$

(5) $\tilde{w} \in \varphi(\mathfrak{M})$.

Ввиду этого $\bar{\Sigma}$ порождает $\varphi(\mathfrak{M})$. Таким образом, $\varphi(\mathfrak{M})$ есть также п. Ш. множество.

Нам осталось еще разобрать тот случай, когда A является рабочим алфавитом Σ. Положим $\bar{A} := A \cup \{\S\}$ и построим с. Ш. $\bar{\Sigma}$ с рабочим алфавитом $\bar{A}$, порождающую $\mathfrak{M}$ (см. 4.10). Изложенное выше доказательство можно полностью перенести на этот случай, если заменить в нем Σ на $\bar{\Sigma}$.

Положим

$$\bar{\Phi} := (\bar{A}, \{v_1, \ldots, v_k\}, \{p_1, \ldots, p_{l+1}\}, \bar{S}),$$

$$\text{где } \bar{S}_i := S_i\ (1 \leqslant i \leqslant l) \text{ и } \bar{S}_{l+1} := 1,$$

$$\bar{\Pi} := \{p_{l+1}\} \cup \{p_{l+1}v_1 \to p_{l+1}v_1 a : a \in A\} \cup \cup \{p_{l+1}v_1 \to \ldots \to p_{l+1}v_k \to \alpha : \alpha \in \Pi\},$$

$$\bar{\Sigma} := \Sigma(\bar{\Phi}, \bar{\Pi}).$$

Тогда можно сначала для $w \in \Omega(\bar{A})$ показать, что

4.9. $\bar{\Sigma} \vdash p_{l+1}w$ *тогда и только тогда, когда* $w \in \Omega(A)$.

По поводу импликации справа налево см. пример 4.7 (1); обратное утверждение доказывается индукцией по длине вывода $p_{l+1}w$ относительно $\bar{\Sigma}$.

Далее для $(w_1, \ldots, w_n) \in \Omega^n(\bar{A})$ имеет место утверждение

4.10. $\bar{\Sigma} \vdash p_1w_1; \ldots; w_n$ *тогда и только тогда, когда* $(w_1, \ldots, w_n) \in \Omega^n(A)$ *и* $\Sigma \vdash p_1w_1; \ldots; w_n$.

А именно, если $(w_1, \ldots, w_n) \in \Omega^n(\bar{A})$ и $\mathfrak{A}$ есть вывод $p_1w_1; \ldots; w_n$ относительно $\bar{\Sigma}$, то, опустив те члены $\mathfrak{A}$, которые содержат p_{l+1}, мы получим вывод относительно Σ, оканчивающийся формулой $p_1w_1; \ldots; w_n$. Отсюда следует, что

$$\Sigma \vdash p_1w_1; \ldots; w_n \quad \text{и} \quad (w_1, \ldots, w_n) \in \Omega^n(A).$$

Обратно, если $(w_1, \ldots, w_n) \in \Omega^n(A)$ и $\Sigma \vdash p_1w_1; \ldots; w_n$, то каждый вывод формулы $p_1w_1; \ldots; w_n$ относительно Σ переходит в вывод $p_1w_1; \ldots; w_n$ относительно $\bar{\Sigma}$. Необходимые доказательства могут быть проведены в обе стороны индукцией по длине вывода, причем в них существенно используется 4.9.

Прежде чем перейти к выяснению связи, существующей между понятиями перечислимости по Шмульяну и по Тьюрингу, нам хотелось бы по крайней мере упомянуть о некоторых других существенных уточнениях понятия исчисления.

4. Специальные системы Шмульяна

4.11. Определение. Пусть $\Phi = (A, V, P, S)$ есть формальный базис и Π — конечное множество Φ-формул. Тогда $\Sigma := \Sigma(\Phi, \Pi)$ называется *канонической системой Поста* в том и только в том случае, когда

(1) $P = \{p_1\}$ и $S_1 = 1$;

(2) Σ обладает по крайней мере одной аксиомой и аксиомы Σ *не содержат* переменных;

(3) если α — одно из конечных заключений Σ, то в каждую атомарную подформулу α входит какая-нибудь переменная, но только в том случае, если *эта же переменная* входит и в самую правую из атомарных подформул α.

Канонические системы Поста, в которых, кроме того, исключен предикат p_1, были в несколько иной форме введены Постом в [12]; они являются одним из важнейших уточнений понятия исчисления.

4.12. Определение. Пусть $\mathfrak{M} \subset \Omega(A)$. Множество $\mathfrak{M}$ называется *перечислимым по Посту* тогда и только тогда, когда $\mathfrak{M}$ пусто или когда существует каноническая система Поста $\Sigma = \Sigma(\Phi, \Pi)$ с рабочим алфавитом A', содержащим A, такая, что для всех $w \in \Omega(A')$ включение $w \in \mathfrak{M}$ имеет место тогда и только тогда, когда $w \in \Omega(A)$ и $\Sigma \vdash p_1 w$.

Перечислимость по Посту и перечислимость по Шмульяну (для множеств слов) — эквивалентные понятия. Это следует, например, из эквивалентности обоих этих понятий понятию перечислимости по Тьюрингу. Эквивалентность перечислимости по Тьюрингу перечислимости по Шмульяну мы докажем в § 5; аналогичная эквивалентность для перечислимости по Посту следует, например, из того, что уже перечислимость, определяемая с помощью *квази-*

стем Туэ (ср. 4.14), эквивалентна перечислимости по Тьюрингу. (В связи с этой последней эквивалентностью см., например, работы Брауэра и Индермарка [1], стр. 101 и далее, или Дэвиса [5], стр. 81 и далее.)

Класс множеств, перечислимых по Посту, *не станет более узким*, если квантор существования в 4.12 ограничить следующими классами специальных канонических систем Поста (мы отказываемся при этом от введения предиката p_1, чтобы приблизиться к обычному способу изложения):

4.13. *Нормальными системами Поста* — каноническими системами Поста, которые содержат *ровно одну* аксиому и все остальные заключения которых имеют вид $wv_1 \rightarrow v_1w'$ (и тем самым содержательно они допускают переход от слова, начинающегося с w, к другому слову, получаемому из первого вычеркиванием начала w и присоединением w'; см. в связи с этим работу Поста [12]);

4.14. *Квазисистемами Туэ* — каноническими системами Поста, которые содержат *ровно одну* аксиому и все остальные заключения которых имеют вид $v_1wv_2 \rightarrow v_1w'v_2$ (и тем самым содержательно они допускают переход от слова, частью которого является w, к некоторому другому, в котором w заменено словом w').

Квазисистемы Туэ, которые наряду с заключением $\alpha \rightarrow \beta$ содержат также заключение $\beta \rightarrow \alpha$, называются *системами Туэ*. Системы Туэ играют некоторую роль в *теории групп* при представлении групп с помощью *образующих* и *определяющих соотношений* (ср., скажем, Хермес [9], стр. 147 и дальше[1])). Название «системы Туэ» восходит к Посту. Оно воздает должное одной работе Туэ 1914 г., посвященной таким системам.

§ 5. Перечислимость по Шмульяну и Тьюрингу

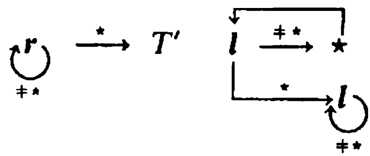
В доказательстве того, что каждое п. Ш. множество является п. Т. множеством и наоборот, мы можем ввиду 3.4(а) и 4.8 ограничиться множествами слов.

---

[1]) Или книгу Кроуэлла и Фокса [19], стр. 62 и далее.— *Прим. перев.*

1. Перечислимость по Шмульяну множеств, перечислимых по Тьюрингу

Пусть $\mathfrak{M} \subset \Omega(A)$ и $\mathfrak{M}$ есть п. Т. множество. Тогда, согласно 3.3, существует в. Т. функция f из $\Omega(A)$, для которой $\mathrm{Def}\, f = \mathfrak{M}$. Пусть м. Т. T' *нормированно* вычисляет f над рабочим алфавитом $A' = \{a_1, \ldots, a_n\}$ (содержащим A). Мы перейдем к м. Т. T с рабочим алфавитом A', таблица которой получается из таблицы для машины



если увеличить индексы всех состояний на 1 и выше первой строки написать строки $q_0 a_i a_i q_1$ для всех i, $0 \leqslant i \leqslant n$. Тогда имеет место следующее утверждение:

5.1. (a) Если $w \in \mathfrak{M}$, то после применения к записи *перед* w машина T останавливается *перед* w в записи $\bigstar w \bigstar \ldots$ (т. е. последовательность конфигураций, начинающаяся с $\bigstar {}^{q_0}w \bigstar \ldots$, обрывается на конфигурации вида $\bigstar {}^{q}w \bigstar \ldots$).

(b) Если $w \in \Omega(A) \setminus \mathfrak{M}$, то после применения к записи *перед* w машина T *не останавливается*.

(c) *Только в начале* вычисления T находится в состоянии q_0 (т. е. в каждой последовательности конфигураций, открывающейся некоторой начальной конфигурацией, только в нулевой конфигурации встречается состояние q_0).

Теперь мы построим некоторую с. Ш. и покажем, что она порождает множество $\mathfrak{M}$. Предположим, что T обладает состояниями $q_0, \ldots, q_m$. Мы определим

(1) $\Phi := (\{a_1, \ldots, a_{n+m+3}\}, \{v_1, v_2\}, \{p_1, p_2\}, S)$, где $S := 1, 1$. Мы будем в дальнейшем часто писать $\underline{a}_i$ вместо a_i $(1 \leqslant i \leqslant n)$, $\overline{q}_i$ вместо a_{n+1+i} $(0 \leqslant i \leqslant m)$ и $\overline{a}_0$ вместо a_{n+m+2}.

(2) П состоит из следующих Ф-формул (их объяснение содержится в заключительных замечаниях):

R 1.1 $p_2 \overline{q}_0 \overline{a}_0$;

R 1.2 $\boldsymbol{p}_2\bar{q}_0\bar{a}_0\boldsymbol{v}_2 \to \boldsymbol{p}_2\bar{q}_0\bar{a}_0\bar{a}\boldsymbol{v}_2$ при $a \in A$;

и далее для всех a, $b \in A' \cup \{a_0\}$ и $q \in \{q_0, \ldots, q_m\}$ имеем

R 2.1 $\boldsymbol{p}_2\boldsymbol{v}_1\bar{q}\bar{a}\boldsymbol{v}_2 \to \boldsymbol{p}_2\boldsymbol{v}_1\bar{q}'\bar{a}'\boldsymbol{v}_2$,
если $qaa'q'$ есть строка таблицы T;

R 2.2.1 $\boldsymbol{p}_2\boldsymbol{v}_1\bar{q}\bar{a} \to \boldsymbol{p}_2\boldsymbol{v}_1\bar{a}\,\bar{q}'\bar{a}_0$ и

R 2.2.2 $\boldsymbol{p}_2\boldsymbol{v}_1\bar{q}\,\bar{a}\,\bar{b}\,\boldsymbol{v}_2 \to \boldsymbol{p}_2\boldsymbol{v}_1\bar{a}\,\bar{q}'\bar{b}\,\boldsymbol{v}_2$,
если $qarq'$ есть строка таблнцы T;

R 2.3.1 $\boldsymbol{p}_2\boldsymbol{v}_1\bar{a}\,\bar{q}\bar{a}_0 \to \boldsymbol{p}_2\boldsymbol{v}_1\bar{q}'\bar{a}$ и

R 2.3.2 $\boldsymbol{p}_2\boldsymbol{v}_1\bar{b}\bar{a}_0\bar{a}\,\boldsymbol{v}_2 \to \boldsymbol{p}_2\boldsymbol{v}_1\bar{q}'\bar{b}\bar{a}_0\bar{a}\,\boldsymbol{v}_2$,
если qa_0lq' есть строка таблицы T;

R 2.3.3 $\boldsymbol{p}_2\boldsymbol{v}_1\bar{b}\,\bar{q}\,\bar{a}\,\boldsymbol{v}_2 \to \boldsymbol{p}_2\boldsymbol{v}_1\bar{q}'\bar{b}\,\bar{a}\,\boldsymbol{v}_2$,
если $a \neq a_0$ и $qalq'$ есть строка таблицы T;

R 3 $\boldsymbol{p}_2\boldsymbol{v}_1\bar{q}\bar{a}_0\boldsymbol{v}_2 \to \boldsymbol{p}_1\boldsymbol{v}_1\boldsymbol{v}_2$,
если $\boldsymbol{s}$ есть действие в начинающейся с символов qa_0 строке таблицы T.

(3) $\Sigma := \Sigma(\Phi, \Pi)$.

Содержательные соображения, которые леглн в основу построения этих заключений и которыми мы будем руководствоваться в остальной части доказательства, таковы: каждой конфигурации

$$a_0 \ldots a_j^q \ldots a_i \ldots,$$

где i — наименьшее из чисел $l \geqslant j$, для которых $a_k = a_0$, когда $k > l$ (тем самым $a_0 \ldots a_i$ есть описание наименьшего отрезка ленты, который содержит текущую рабочую ячейку и все ячейки с собственными буквамн), сопоставляется так называемое *конфигурационное слово*

$$\bar{a}_0 \ldots \bar{a}_{j-1}\bar{q}\bar{a}_j \ldots \bar{a}_i.$$

Тогда система Σ допускает вывод тех Φ-формул $\boldsymbol{p}_2 w$ из совокупности всех атомарных Φ-формул, начинающихся символом $\boldsymbol{p}_2$, для которых w есть конфигурационное слово некоторой конфигурации, пробегаемой машнной T после ее применения к записн *перед* некоторым словом из $\Omega(A)$. Заключения R1 служат для вывода начальных конфигураций, заключения R2 обеспечивают переход к следующей конфигурации. Мы опишем это положение вещей более точно (символом w обозначаются далее слова над $\{a_1, \ldots, a_{n+m+2}\}$):

5.2. $\Sigma \vdash p_2 w$ тогда и только тогда, когда w есть конфигурационное слово некоторой конфигурации, пробегаемой машиной T после применения *перед* некоторым словом над A.

Предположим сначала, что 5.2 доказано. Тогда следующие утверждения эквивалентны:

(1) $\Sigma \vdash p_1 w$.

(2) Существуют w_1, w_2 и q, такие, что $\Sigma \vdash p_2 w_1 q \overline{a}_0 w_2$, s есть действие строки таблицы T, начинающейся с символов qa_0, и $w = w_1 w_2$. (В том случае,когда $\Sigma \vdash p_1 w$, Ф-формула $p_1 w$ обязательно выводима по R3!)

(3) Существуют w_1, w_2 и q, такие, что $w = w_1 w_2$ и $w_1 \overline{q}\, \overline{a}_0 w_2$ есть конфигурационное слово некоторой конфигурации, которую пробегает машина T после применения *перед* каким-то словом над A и у которой нет следующей конфигурации, так как имеет место машинный останов T (и, таким образом, согласно 5.1 (a), (b), $w_1 = \square$, $w_2 = w$ и $w_2 \in \Omega(A)$). (Эквивалентность (2) и (3) следует из 5.2!)

(4) Существует слово w' над A, такое, что T, примененная *перед* w', останавливается перед w.

(5) $w \in \mathfrak{M}$.

(Для доказательства эквивалентности (4) и (5) воспользуемся утверждением 5.1 (a), (b)!)

Тем самым доказано, что Σ порождает $\mathfrak{M}$. Отсюда следует

5.3. Теорема. *Если* $\mathfrak{M} \subset \Omega(A)$ *и* $\mathfrak{M}$ *есть п. Т. множество, то* $\mathfrak{M}$ *есть п. Ш. множество.*

Теперь обратимся к доказательству 5.2.

Сначала мы докажем импликацию слева направо, пользуясь индукцией по длине $l(w)$ вывода $p_2 w$ минимальной длины.

Предположим (*база индукции*!), что $l(w) = 1$. Тогда $p_2 w$ с необходимостью есть Ф-подстановка R 1.1 и, таким образом, $w = \overline{q}_0\, \overline{a}_0$. Но $\overline{q}_0\, \overline{a}_0$ есть конфигурационное слово начальной конфигурации, когда T применяется *перед* пустым словом.

Шаг индукции. Пусть $l(w) > 1$. Тогда $\boldsymbol{p}_2 w$ должно быть результатом применения правила Modus Ponens к Ф-подстановке $\alpha \to \beta$ заключения вида R 1.2 или R 2 и α. Мы рассмотрим два типичных случая.

(a) Пусть $\alpha \to \beta$ есть Ф-подстановка заключения вида R 1.2. Тогда существуют w_2 и $a \in A$, такие, что

$$\alpha = \boldsymbol{p}_2 \bar{\boldsymbol{q}}_0 \bar{\boldsymbol{a}}_0 w_2, \quad \beta = \boldsymbol{p}_2 w = \boldsymbol{p}_2 \bar{\boldsymbol{q}}_0 \boldsymbol{a}_0 \bar{a} w_2,$$
$$\Sigma \vdash \boldsymbol{p}_2 \boldsymbol{q}_0 \bar{\boldsymbol{a}}_0 w_2 \quad \text{и} \quad l(\bar{\boldsymbol{q}}_0 \boldsymbol{a}_0 w_2) < l(w).$$

Из индуктивного предположения следует, что $\bar{\boldsymbol{q}}_0 \bar{\boldsymbol{a}}_0 w_2$ есть конфигурационное слово для некоторой конфигурации, пробегаемой машиной T, когда T применена *перед* подходящим словом над A. Согласно 5.1 (c), эта конфигурация является нулевой конфигурацией в такой конфигурационной последовательности. Отсюда следует, что $w_2 \in \Omega(A)$, а также и $\bar{a} w_2 (= a w_2) \in \Omega(A)$, и w есть конфигурационное слово начальной конфигурации при применении T *перед* $\bar{a} w_2$.

(b) Пусть $\alpha \to \beta$ есть Ф-подстановка заключения вида R 2.1. Тогда существуют слова w_1, w_2 и строка $qaa'q'$ таблицы T, такие, что $\alpha = \boldsymbol{p}_2 w_1 \bar{q} \bar{a} w_2$ и $\beta = \boldsymbol{p}_2 w = \boldsymbol{p}_2 w_1 \bar{q}' \bar{a}' w_2$. Ввиду неравенства $l(w_1 \bar{q} \bar{a} w_2) < l(w)$ и по индуктивному предположению наше утверждение непосредственно следует из того факта, что переходу от $w_1 \overline{qa} w_2$ к $w_1 \bar{q}' \bar{a}' w_2$ соответствует переход (сопровождаемый выполнением соответствующего указания о печати) от конфигурации, описываемой словом $w_1 \overline{qa} w_2$, к следующей за ней конфигурации.

Теперь об импликации справа налево в 5.2. Мы докажем ее индукцией по номеру соответствующей w конфигурации в некоторой конфигурационной последовательности, которую пробегает машина T, примененная к записи *перед* некоторым словом над A. Если слово w описывает некоторую *начальную* в этом смысле *конфигурацию*, то очевидно, что $\boldsymbol{p}_2 w$ может быть выведена с помощью заключения вида R 1. Если же (*шаг индукции*!) w есть конфигурационное слово конфигурации, следующей за некоторой другой в конфигурационной последовательности рассматриваемого вида, то к этой предшествующей конфигурации с конфигурационным словом w' применимо предположение индукции. Итак, $\Sigma \vdash p_2 w'$. Если переход к соответствующей w конфигурации состоит в выполнении *указания о печати*, то $p_2 w' \to p_2 w$ есть Ф-подстановка заключения вида R 2.1; если требуемое действие есть r, то $p_2 w' \to p_2 w$ есть Ф-подстановка заключения вида R 2.2.1 в том случае, когда ни одна из ячеек, лежащих правее текущей рабочей ячейки предыдущей конфигурации, не содержит собственной буквы; в противном же случае $p_2 w' \to p_2 w$ есть Ф-подстановка заключения вида R 2.2.2. Соответственно, когда действие есть l, нужно рассмотреть Ф-подстановку заключения вида R 2.3. Применение правила Modus Ponens к $p_2 w' \to p_2 w$ и $p_2 w'$ дает нам в каждом из обсуждаемых случаев $\Sigma \vdash p_2 w$.

Тем самым 5.2 доказано.

2. Перечислимость по Тьюрингу множеств, перечислимых по Шмульяну

Мы дадим в этом пункте набросок доказательства следующей теоремы:

5.4. Теорема. *Если $\mathfrak{M} \subset \Omega(A)$ и $\mathfrak{M}$ есть п. Ш. множество, то $\mathfrak{M}$ есть п. Т. множество.*

Мы будем исходить из п. Ш. подмножества $\mathfrak{M} \subset \Omega(A)$. Пусть $\Sigma = \Sigma(\Phi, \Pi)$ есть порождающая $\mathfrak{M}$ с. Ш. с рабочим алфавитом A', содержащим A. Пусть $\{v_1, \ldots, v_k\}$ есть алфавит переменных базиса Ф. Согласно МТВФ II, п.9 § 3, существуют в. Т. функции $f_1, \ldots, f_k$, отображающие $\mathbf{N}$ в $\Omega(A')$, так что $\Omega^k(A') = \{f_1(n), \ldots, f_k(n)) : n \in \mathbf{N}\}$.

Пусть $\alpha_1, \ldots, \alpha_m$ — заключения Σ. Для данных $i \in \{1, \ldots, m\}$ и $n \in \mathbf{N}$ обозначим через α_i^n результат подстановки в α_i соответствующих функций $f_j(n)$ вместо всех входящих в α_i переменных v_j. Легко проверить, что функции $g_1, \ldots, g_m$ с $\operatorname{Def} g_i = \mathbf{N}$ и $g_i(n) = \alpha_i^n$ для $n \in \mathbf{N}$ являются в. Т. функциями и что каждая Ф-подстановка некоторого заключения Σ встречается среди Ф-формул $g_i(j)$. (Здесь мы не принимаем во внимание неопределенность, которую можно устранить простым переименованием и которая связана с тем, что символ ;, переменные и предикаты могут не принадлежать алфавиту, который мы ввели.)

Теперь мы опишем блок-схему процедуры вычисления функции из $\Omega(A)$ с областью определения, состоящей из Ф-слов w, для которых $\Sigma \vdash p_1 w$, т. е. $w \in \mathfrak{M}$.

Нетрудно, хотя и довольно канительно, построить м. Т., моделирующую эту процедуру, и тем самым охарактеризовать $\mathfrak{M}$, согласно 3.3, как п. Т. множество.

Предположим, что задано $w \in \Omega(A)$. Будем действовать согласно следующему плану:

1) Положим $n = 0$.

2) Построим Ф-подстановки $g_i(j)$ для всех i, j, $1 \leqslant i \leqslant m$, $0 \leqslant j \leqslant n$.

3) Определим все *атомарные* Ф-формулы, получаемые из этих Ф-подстановок с использованием правила Modus Ponens (например, вычеркивая, пока это возможно, уже полученные ранее собственные атомарные подформулы, начиная с самых левых).

4) Сравним с $p_1 w$ все полученные в 3) атомарные Ф-формулы, одну за другой. Если при этом хотя бы однажды мы получим равенство, то далее действуем согласно 5), в противном случае — согласно 6).

5) Прерываем процедуру с результатом, равным w.

6) Увеличим число n на 1 и действуем далее согласно 2).

Если процедура, описанная в 1) — 6), обрывается, то, конечно, $\Sigma \vdash p_1 w$. Обратно, пусть $\Sigma \vdash p_1 w$ и $\mathfrak{A}$ есть вывод для $p_1 w$ относительно Σ. Тогда $\mathfrak{A}$ останется выводом, если все члены, полученные правилом подстановки, собрать в начале вывода. Существует такое n, для которого все эти члены находятся среди членов $g_i(j)$, где $1 \leqslant i \leqslant m$ и $0 \leqslant j \leqslant n$, и $p_1 w$ выводимо из этих членов по правилу Modus Ponens. Тогда вышеописанная процедура, примененная к w, обрывается самое позднее после $(n+1)$-го применения 4).

Этим наброском мы завершаем доказательство 5.4.

3. Неразрешимая система Шмульяна

Мы хотели бы из всего ранее доказанного вывести одно следствие, существенно используемое в § 6. Согласно 3.12, мы можем эффективно задать м. Т. T' с рабочим алфавитом A', содержащим A, которая обладает следующими свойствами:

$\mathfrak{M}(T', A, 1)$ есть п. Т. множество (ср. 3.5);

$\Omega(A) \setminus \mathfrak{M}(T', A, 1)$ не есть п. Т. множество;

T' нормированно вычисляет определяемую ею функцию f из $\Omega(A)$ в $\Omega(A)$, так что $\mathrm{Def} f = \mathfrak{M}(T', A, 1)$.

С множеством $\mathfrak{M} := \mathfrak{M}(T', A, 1)$, машиной T' или функцией f мы можем теперь действовать точно так же, как и при доказательстве 5.3 с $\mathfrak{M}$, T' или f (ср. стр. 119 и далее). Если воспользоваться обозначениями стр. 119, то это означает, что из T' мы можем сначала *эффективно* построить м. Т. T и, наконец, с. Ш. Σ, порождающую $\mathfrak{M}(T', A, 1)$. Система Σ_0 получается из Σ, если в заключениях R 1 — R 3 для Σ заменить $\boldsymbol{p}_2$ на $\boldsymbol{p}_1$. Воспользовавшись опять соответствующими обозначениями (w есть Ф-слово), получим

5.5. $\Sigma \vdash \boldsymbol{p}_1 w$ *тогда и только тогда, когда* $\Sigma_0 \vdash \boldsymbol{p}_1 w$ *и* w *не содержит* $\bar{q}$.

Импликация слева направо тривиальна, так как Σ порождает $\mathfrak{M}(T', A, 1)$. Для доказательства обратной импликации нужно лишь заметить, что любой вывод относительно Σ_0 переходит в некоторый вывод относительно Σ, если в первом из них во всех его атомарных подформулах, содержащих $\bar{q}$, заменить $\boldsymbol{p}_1$ на $\boldsymbol{p}_2$.

Мы утверждаем далее, что

5.6. *Множество* $\{w$: *заключение* $\boldsymbol{p}_1 w$ *невыводимо, т. е. не* $\Sigma \vdash \boldsymbol{p}_1 w\}$ *не перечислимо по Шмульяну.*

Доказательство от противного. Если бы $\{w$: не $\Sigma_0 \vdash \boldsymbol{p}_1 w\}$ было п. Ш. множеством, то, согласно 5.4, оно было бы также и п. Т. множеством. Так как $\Omega(A)$ есть п. Т. множество, то, согласно 3.7, $\{w$: не $\Sigma_0 \vdash \boldsymbol{p}_1 w\} \cap \Omega(A)$ также будет п. Т. множеством. Так как, согласно 5.5, $\Sigma_0 \vdash \boldsymbol{p}_1 w$ для $w \in \Omega(A)$ имеет место тогда и только тогда, когда $\Sigma \vdash \boldsymbol{p}_1 w$, то отсюда следует перечислимость по Тьюрингу множества $\{w : w \in \Omega(A)$ и не $\Sigma \vdash \boldsymbol{p}_1 w\}$. Так как Σ порождает $\mathfrak{M}(T', A, 1)$, то $\Omega(A) \setminus \mathfrak{M}(T', A, 1)$ будет п. Т. множеством, что является противоречием.

Система Шмульяна, для которой имеет место аналог 5.6, называется *неразрешимой*. Тем самым доказана такая

5.7. Теорема. *Можно эффективно задать неразрешимую с. Ш.* (эффективно построив Ф и П).

(Так называемая *проблема тождества слов в теории групп* (ср. Хермес [9]) тесно связана с вопросом о существовании специальных неразрешимых *систем Туэ*. Такие неразрешимые системы были впервые построены П. С. Новиковым (1955) и Буном (1957).)

В заключениях рассмотренной выше с. Ш. Σ_0 встречается единственный предикат: p_1. Откажемся от введения p_1 и изменим соответственно все синтаксические понятия, такие, как *формула*, *правило*, *заключение*, *вывод* и т. д.; обозначив через Σ возникшую в результате систему для случая $A=\{|\}$ и через A — рабочий алфавит Σ, получим

5.8. (a) Система Σ (точнее, заключения системы Σ) может быть задана эффективно.

(b) Σ содержит точно одну аксиому. Неатомарные заключения Σ имеют вид $v_1wv_2 \to v_1w'v_2$ или $v_1w \to v_1w'$, или $wv_2 \to w'v_2$ со словами w, w' над A.

(c) $\{w : w \in \Omega(A)$ и не $\Sigma \vdash w\}$ не является п. Ш.

4. Заключительные замечания

Мы ввели уже несколько точных определений перечислимости и выяснили более или менее подробно, что эти определения эквивалентны между собой. Вместо того чтобы говорить теперь о *перечислимости в смысле одного из этих эквивалентных друг другу уточнений*, предпочтительнее говорить *о рекурсивной перечислимости* или *общерекурсивной перечислимости*. Тем самым все теоремы § 3—5 останутся справедливыми, если мы заменим в них п. Т. или п. Ш. на «рекурсивно перечислимый».

§ 6. Неперечислимость множества истинных арифметических высказываний и неразрешимость арифметики

Мы завершим наше изложение доказательством *неперечислимости* одного интересного с математической точки зрения множества — *множества истинных арифметических высказываний*. Прежде чем изложить соображения, лежащие в основе доказательства, рассмотрим подробнее арифметические выражения и высказывания.

1. Арифметические выражения и высказывания

Мы определим совокупность высказываний с помощью с. Ш. $\sum$. Пусть $\Phi := (A, V, P, S)$; пусть при этом

$$A = \{|, \mathbf{O}, +, \times, \neg, \wedge, \bigwedge, =, (,)\},$$

где обозначения выбраны содержательным образом (символы $+$ и $\times$ должны напоминать соответственно о сложении и умножении; символы $\neg$, $\wedge$, $\bigwedge$ — об употребительных логических обозначениях соответственно для *не*, *и*, *для всех*; знак $=$ — о знаке равенства).

$$V = \{\xi, \mathbf{s}, \mathbf{t}, \alpha, \beta\},$$
$$P = \{\textit{Переменная}, \textit{Терм}, \textit{Выражение}\}^{1}).$$

Присоединяя сюда описанное ниже множество П Ф-формул, положим $\sum := \Sigma(\Phi, \Pi)$.

Заключения системы $\sum$ (т. е. элементы П) разбиваются на *три* группы. Заключения первой группы служат для получения так называемых *числовых переменных*, второй — для получения так называемых *числовых термов*, а третьей — для получения так называемых *арифметических выражений*.

6.1. (1) *Переменная* $\mathbf{O}$,
Переменная $\xi \to$ *Переменная* $\xi|$,
(2) *Переменная* $\xi \to$ *Терм* ξ,
Терм $\mathbf{s} \to$ *Терм* $\mathbf{t} \to$ *Терм* $(\mathbf{s} + \mathbf{t})$,
Терм $\mathbf{s} \to$ *Терм* $\mathbf{t} \to$ *Терм* $(\mathbf{s} \times \mathbf{t})$,
(3) *Терм* $\mathbf{s} \to$ *Терм* $\mathbf{t} \to$ *Выражение* $\mathbf{s} = \mathbf{t}$,
Выражение $\alpha \to$ *Выражение* $\neg\alpha$,
Выражение $\alpha \to$ *Выражение* $\beta \to$ *Выражение* $(\alpha \wedge \beta)$,
Выражение $\alpha \to$ *Переменная* $\xi \to$ *Выражение* $\bigwedge \xi\alpha$.

В качестве обозначений для *числовых переменных*, т. е. элементов множества $\{w : \sum \vdash \textit{Переменная } w\}$, мы исполь-

[1]) Здесь *Переменная* есть содержательный предикатный символ. Аналогичные символы используются и дальше; они являются русскими эквивалентами соответствующих немецких терминов.—*Прим. перев.*

зуем буквы ξ, η, ...; примеры числовых переменных: O, $O|||$.

В качестве обозначений для *числовых термов*, т. е. элементов множества $\{w: \sum \vdash$ *Терм* $w\}$, мы используем буквы s, t, ...; примеры числовых термов:

$$O, \qquad (O+O|), \qquad (O\times(O+O)).$$

В качестве обозначений для *арифметических выражений*, т. е. элементов множества $\{w: \sum \vdash$ *Выражение* $w\}$, мы используем буквы α, β, ... ; примеры арифметических выражений: $O=O|$,

$$(O=O|\wedge\bigwedge O(O=(O\times O|)\wedge\neg O=(O+O))).$$

Теперь мы уточним, что называется *свободным вхождением* числовой переменной ξ в выражение α. Содержательно это означает, что место, которое занимает ξ в α, не входит в *область действия* $\bigwedge\xi$. Например, O входит свободно в $(\bigwedge OO=O|\wedge(O+O)=O)$, но не в $\bigwedge OO=O|$.

Мы дадим индуктивное определение для всех возможных схем получения арифметических выражений согласно группе заключений 6.1(3).

6.2. ξ *входит свободно в* $s=t$ тогда и только тогда, когда ξ входит в s или t [1]).

ξ *входит свободно в* $\neg\alpha$ тогда и только тогда, когда ξ *входит свободно в* α.

ξ *входит свободно* в $(\alpha\wedge\beta)$ тогда и только тогда, когда ξ *входит свободно в* α или когда ξ *входит свободно в* β.

ξ *входит свободно в* $\bigwedge\eta\alpha$ тогда и только тогда, когда ξ *входит свободно в* α и отлично от η.

Нетрудно вместо 6.2 дать исчислительное и тем самым эффективное определение свободного вхождения. Можно было бы, например, так пополнить с. Ш. $\sum$ введением добавочного двуместного предиката *Свободная* и соответствующих заключений, чтобы формула *Свободная* $w_1; w_2$

[1]) Это означает, что ξ входит в s или t как слово, причем непосредственно справа от него не стоит знак | (штрих). Мы оставляем читателю задачу уточнения понятия вхождения числовой переменной в числовой терм; это можно сделать, например, с помощью индуктивного определения.

была выводима тогда и только тогда, когда w_1 — числовая переменная, w_2 — арифметическое выражение и w_1 свободно входит в w_2.

6.3. Предположим, что α — некоторое арифметическое выражение; α называется *арифметическим высказыванием* тогда и только тогда, когда ни одна числовая переменная не входит свободно в α.

2. Значения. Арифметические предикаты

Каждому *арифметическому выражению* можно сопоставить некоторое *высказывание над множеством натуральных чисел*, в котором всем свободно входящим в это выражение числовым переменным отвечают числовые параметры. Высказывание может быть *истинным* относительно одних значений числовых параметров и *ложным* относительно других. *Арифметические* высказывания соответствуют *не содержащим параметров* высказываниям над множеством натуральных чисел. Они *просто* либо ложны, либо истинны.

Мы уточним это сопоставление. Для каждого арифметического выражения α обозначим через *Свободные* (α) множество всех свободно входящих в α числовых переменных. Пусть $\mathfrak{D}$ есть множество отображений *из* множества числовых переменных в $\mathbf{N}$. Мы назовем элементы $\mathfrak{D}$ *значениями*. В качестве обозначений для значений мы используем буквы $\delta, \ldots$. В качестве обозначений для натуральных чисел мы используем буквы $m, n, \ldots$. Пусть δ_ξ^n — такое значение, которое отличается от δ самое большее тем, что отображает числовую перемеиную ξ в натуральное число n, и для которого, таким образом,

$$\operatorname{Def}\delta_\xi^n = \operatorname{Def}\delta \cup \{\xi\},$$

$$\delta_\xi^n \,|\, (\operatorname{Def}\delta \setminus \{\xi\}) = \delta \,|\, (\operatorname{Def}\delta \setminus \{\xi\}) \quad \text{и} \quad \delta_\xi^n(\xi) = n\,^{1)}.$$

Каждому числовому терму t и каждому значенню δ, для которого *Свободные* $(t = t) \subset \operatorname{Def}\delta$, в соответствии со значениями (по δ) входящих в t числовых переменных

[1]) $\delta \,|\, \mathfrak{N}$, где $\mathfrak{N} \subset \operatorname{Def}\delta$, есть ограничение значения δ на множество $\mathfrak{N}$.— *Прим. перев.*

отвечает число $n(\delta, t)$, которое мы определим индуктивно согласно возможным способам получения числовых термов посредством группы заключений 6.1 (2)[1]).

6.4. Если $\xi \in \mathrm{Def}\,\delta$, то положим $n(\delta, \xi) := \delta(\xi)$. Если *Свободные* $(s \equiv t) \subset \mathrm{Def}\,\delta$, то положим $n(\delta, (s \boldsymbol{+} t)) := n(\delta, s) + n(\delta, t)$ и $n(\delta, (s \times t)) := n(\delta, s) \cdot n(\delta, t)$.

Отсюда следует

6.5. Если *Свободные* $(t \equiv t) \subset \mathrm{Def}\,\delta_1 \cap \mathrm{Def}\,\delta_2$ и $\delta_1 \mid$ *Свободные* $(t \equiv t) = \delta_2 \mid$ *Свободные* $(t \equiv t)$, то $n(\delta_1, t) = n(\delta_2, t)$.

(«Значение» конкретного числового терма, соответствующее некоторому значению δ, зависит, таким образом, лишь от того, как это значение δ отображает *свободно входящие в* t числовые переменные.)

Доказательство получается индукцией в соответствии с индуктивным определением 6.4. Пусть сначала $t = \xi$ и $\xi \in \mathrm{Def}\,\delta_1 \cap \mathrm{Def}\,\delta_2$, $\delta_1(\xi) = \delta_2(\xi)$. Тогда $n(\delta_1, \xi) = \delta_1(\xi) = \delta_2(\xi) = n(\delta_2, \xi)$. Пусть, далее (это есть *шаг индукции*), для $t' := (s \boldsymbol{+} t)$ мы имеем *Свободные* $(t' \equiv t') \subset \mathrm{Def}\,\delta_1 \cap \mathrm{Def}\,\delta_2$ и $\delta_1 \mid$ *Свободные* $(t' \equiv t') = \delta_2 \mid$ *Свободные* $(t' \equiv t')$. Тогда ввиду равенства *Свободные* $(s \equiv s) \cup$ *Свободные* $(t \equiv t) =$ *Свободные* $(t' \equiv t')$ к s, δ_1, δ_2 и t, δ_1, δ_2 применимо индуктивное предположение и мы получаем $n(\delta_1, (s \boldsymbol{+} t)) = n(\delta_1, s) + n(\delta_1, t) = n(\delta_2, s) + n(\delta_2, t) = n(\delta_2, (s \boldsymbol{+} t))$. Тот же порядок действий применим и к умножению.

Теперь для арифметического выражения α и значений δ, когда *Свободные* $(\alpha) \subset \mathrm{Def}\,\delta$, мы индуктивно определим (как в 6.2) отношение «*α выполняется при δ*»:

6.6. (1) Пусть *Свободные* $(s \equiv t) \subset \mathrm{Def}\,\delta$;

$s \equiv t$ *выполняется при* δ тогда и только тогда, когда $n(\delta, s) = n(\delta, t)$.

(2) Пусть *Свободные* $(\neg\alpha) \subset \mathrm{Def}\,\delta$;

$\neg\alpha$ *выполняется при* δ тогда и только тогда, когда α *выполняется при* δ.

---

[1]) Следует проводить строгое различие между знаком $\equiv$ формального языка арифметики и метаязыковым знаком равенства $=$, а также между знаками $\boldsymbol{+}$ и $+$ и т. д.

(3) Пусть *Свободные* $((\alpha \wedge \beta)) \subset \mathrm{Def}\,\delta$;

$(\alpha \wedge \beta)$ *выполняется при* δ тогда и только тогда, когда α *выполняется при* δ и β *выполняется при* δ.

(4) Пусть *Свободные* $(\bigwedge \xi\alpha) \subset \mathrm{Def}\,\delta$;

$\bigwedge \xi\alpha$ *выполняется при* δ тогда и только тогда, когда для всех n выражение α *выполняется при* δ_ξ^n.

В связи с этим отметим, что *Свободные* $(\neg\alpha) =$ *Свободные* (α), *Свободные* $((\alpha \wedge \beta)) =$ *Свободные* $(\alpha) \cup$ *Свободные* (β) и *Свободные* $(\bigwedge \xi\alpha) =$ *Свободные* $(\alpha) \setminus \{\xi\}$.

Теперь аналогично 6.5 и так же просто доказывается

6.7 (теорема о коинциденции). Если *Свободные* $(\alpha) \subset \mathrm{Def}\,\delta_1 \cap \mathrm{Def}\,\delta_2$ и $\delta_1 \mid$ *Свободные* $(\alpha) = \delta_2 \mid$ *Свободные* (α), то α *выполняется при* δ_1 тогда и только тогда, когда α *выполняется при* δ_2.

Выполняется ли арифметическое выражение α при значении δ, зависит, таким образом, только от набора тех чисел δ, которые сопоставляются *в α свободно входящим числовым переменным*. Обозначим значение с пустой областью определения через $\boldsymbol{\delta}$; тогда 6.7 означает, в частности, следующее:

6.8. Пусть α — некоторое арифметическое высказывание (т. е. *Свободные* (α) есть пустое множество). Тогда для произвольного δ имеет место утверждение:

α *выполняется при* δ тогда и только тогда, когда α *выполняется при* $\boldsymbol{\delta}$.

Итак, арифметические высказывания либо выполняются при *всех* значениях, либо не выполняются *ни при каких* значениях. Арифметические высказывания первого вида мы назовем *истинными*, а второго вида — *ложными*.

В дальнейшем мы часто записываем арифметические выражения в форме $\alpha(\xi_1, \ldots, \xi_m)$ для того, чтобы указать, что $\xi_1, \ldots, \xi_m$ являются *различными* числовыми переменными, что в α входят числовые переменные $\xi_1, \ldots, \xi_m$ и только они, что они находятся *на определенных местах* и при этом их *вхождение свободно*. Так как мы употребляем этот способ записи только для тех выражений, для которых мы ранее сформулировали *точное определение* или *эффективную процедуру построения*, то мы можем в связи с этим отказаться от уточнения понятия *вхождения числовой переменной на определенном месте.*

$\alpha(\xi_1, \ldots, \xi_m)$ обозначает m-местное *отношение* $\mathfrak{R}_{\alpha(\xi_1, \ldots, \xi_m)}$ над $\mathbf{N}$ в соответствии с определением:

6.9. $\mathfrak{R}_{\alpha(\xi_1, \ldots, \xi_m)}$ имеет место для набора $(n_1, \ldots, n_m)$ тогда и только тогда, когда $\alpha(\xi_1, \ldots, \xi_m)$ *выполняется при* $(\ldots(\delta_{\xi_1}^{n_1})\ldots)_{\xi_m}^{n_m}$.

Вместо фразы «$\mathfrak{R}_{\alpha(\xi_1, \ldots, \xi_m)}$ имеет место для $(n_1, \ldots, n_m)$» мы будем часто писать $\alpha\ (n_1, \ldots, n_m)$.

Приведем несколько примеров.

6.10. (1) $\alpha(\xi) := (\xi) \equiv (\xi + \xi)$ определяет одноместное отношение, выражающее свойство быть тождественно равным нулю.

(2) $\alpha(\xi) := \neg \bigwedge \eta \neg \xi \equiv (\eta + \eta)$ (при $\xi \neq \eta$) определяет одноместное отношение, выражающее свойство быть четным числом.

(3) $\alpha(\xi_1, \xi_2) := \neg \bigwedge \eta \neg (\eta + \xi_1) \equiv \xi_2$ (при $\xi_1 \neq \eta$, $\xi_2 \neq \eta$) определяет отношение $\leqslant$.

Переходя к доказательству, например, 6.10 (3), рассмотрим, первый и последний члены следующей цепочки попарно эквивалентных высказываний (их эквивалентность следует в основном из 6.6):

(a) $\alpha(\xi_1, \xi_2)$ *выполняется при* $(\delta_{\xi_1}^{n_1})_{\xi_2}^{n_2}$.

(b) Отрицание $\bigwedge \eta \neg (\eta + \xi_1) \equiv \xi_2$ *выполняется при* $(\delta_{\xi_1}^{n_1})_{\xi_2}^{n_2}$.

(c) Не для всех m: $\neg (\eta + \xi_1) \equiv \xi_2$ *выполняется при* $((\delta_{\xi_1}^{n_1})_{\xi_2}^{n_2})_{\eta}^{m}$.

(d) Не для всех m: отрицание $(\eta + \xi_1) \equiv \xi_2$ *выполняется при* $((\delta_{\xi_1}^{n_1})_{\xi_2}^{n_2})_{\eta}^{m}$.

(e) Существует m, такое, что $(\eta + \xi_1) \equiv \xi_2$ *выполняется при* $((\delta_{\xi_1}^{n_1})_{\xi_2}^{n_2})_{\eta}^{m}$.

(f) Существует m, для которого $m + n_1 = n_2$.

(g) $n_1 \leqslant n_2$.

В заключение мы условимся о следующих обозначениях:

6.11. (a) $(\alpha \vee \beta)$ эквивалентно $\neg(\neg \alpha \wedge \neg \beta)$,

(b) $(\alpha \rightarrow \beta)$ эквивалентно $(\neg \alpha \vee \beta)$,

(c) $\bigvee \xi \alpha$ эквивалентно $\neg \bigwedge \xi \neg \alpha$.

Отсюда следует

6.12. (a) Пусть *Свободные* $(\alpha) \cup$ *Свободные* $(\beta) \subset \mathrm{Def}\,\delta$. Тогда

$(\alpha \vee \beta)$ *выполняется при* δ в том и только в том случае, когда α *выполняется при* δ или β *выполняется при* δ;

$(\alpha \to \beta)$ *выполняется при* δ в том и только в том случае, когда (если α *выполняется при* δ, то и β *выполняется при* δ).

(b) Пусть *Свободные* $(\alpha) \setminus \{\xi\} \subset \mathrm{Def}\,\delta$. Тогда $\bigvee \xi\alpha$ *выполняется при* δ в том и только в том случае, когда существует такое n, что α *выполняется при* δ_{ξ}^{n}.

(В связи с 6.12 (a) заметнм, что мы используем союз *или* не в *разделительном* смысле, а служебные слова *если... то...* означают *импликацию Филона*: соответствующее высказывание ложно тогда и только тогда, когда его первая часть истинна, а вторая ложна.)

Для дальнейшего условимся о следующих способах экономии скобок при написании выражений.

(a) Мы будем часто опускать *внешние скобки* выражений.

(b) *В многократных конъюнкциях* $\alpha_1 \wedge \ldots \wedge \alpha_n$ и *многократных дизъюнкциях* $\alpha_1 \vee \ldots \vee \alpha_n$ будет предполагаться расстановка скобок слева направо.

(c) *В числовых термах* мы принимаем обычные правила расстановки скобок в арифметических выражениях (для сложения и умножения).

3. Обзор

Наша цель—доказательство следующей теоремы:

6.13. Теорема. *Множество истинных арифметических высказываний неперечислимо.*

Согласно 2.3, отсюда вытекает

6.14. Теорема о неразрешимости арифметики. *Множество истинных арифметических высказываний неразрешимо.*

Вместо *истинных* высказываний арифметики можно рассматривать также такие высказывания, которые следуют из близкой системы аксиом для натуральных чисел в рамках так называемой *логики предикатов первой сту-*

пени[1]). Если, например, система аксиом включает в себя *систему аксиом Пеано*, в которой *аксиома индукции*, не допускающая формулировки на этом языке, заменена *схемой* выражений вида

$$\bigwedge \eta_1 \ldots \bigwedge \eta_n ((\alpha(0, \eta_1, \ldots, \eta_n) \wedge \bigwedge \xi(\alpha(\xi, \eta_1, \ldots, \eta_n) \to \\ \to \alpha(\xi + 1, \eta_1, \ldots, \eta_n))) \to \bigwedge \xi \alpha(\xi, \eta_1, \ldots, \eta_n)),$$

а также обычные рекурсивные соотношения для сложения и умножения, то становится справедливым утверждение, аналогичное 6.14 и восходящее к Чёрчу [4]. В этом случае говорят о так называемой *арифметике Пеано*. Аналог теоремы 6.13 для арифметики Пеано *не выполняется*. Обзор дальнейших результатов, связанных с этой темой, можно найти в книге Тарского, Мостовского, Робинсона [17]. Теорема 6.14 была впервые доказана Тарским [16].

Для доказательства 6.13 мы предложим следующий путь. Будем исходить из системы Σ, определенной в 5.8. Каждому слову w над рабочим алфавитом A из Σ мы эффективным образом сопоставим определенные натуральные числа, так называемые *кодирующие числа* или *числовые коды* слова w. По числовому коду для w мы можем эффективно восстановить w. Затем мы конструируем арифметическое выражение *Невывод* (ξ), обладающее следующими свойствами: *Невывод* (n) истинно тогда и только тогда, когда n есть числовой код некоторого *невыводимого* относительно Σ слова над A. Отсюда мы получаем (ср. 6.49) эффективные арифметические высказывания α^n для всех $n \in \mathbf{N}$, для которых справедливо следующее утверждение:

α^n истинно тогда и только тогда, когда n есть числовой код некоторого невыводимого относительно Σ слова над A.

Ввиду эффективности всех конструкций отсюда следует, что если бы множество всех истинных арифметических высказываний было перечислимым, то перечислимым было бы и множество истинных высказываний из числа высказываний α^n, а значит, и множество всех невыводимых

---

[1]) Описание логики предикатов первой ступени дано в следующей статье этой книги: «Проблема разрешимости и игра «домино»» (см. стр. 150 и далее).— *Прим. перев.*

относительно Σ слов над A. Но это противоречило бы неразрешимости Σ.

Здесь и далее мы пользуемся понятиями вычислимости и перечислимости лишь в их наглядном истолковании. Мы хотели бы, однако, отметить, что в принципе все доказательства,— возможно, после довольно значительных технических усилий,— могут быть также проведены и для точно определенных понятий. Сохраняя и в дальнейшем эвристическую форму изложения, мы будем существенно опираться на тот факт, что понятие перечислимости может быть адекватно уточнено, например, с помощью систем Шмульяна. Действительно, применяя 5.8, мы предполагаем известным тот факт, что множество слов над A, невыводимых относительно Σ, неперечислимо; таким образом, мы пользуемся тем, что множество, перечислимое *в интуитивном смысле*, перечислимо и *по Шмульяну*.

Для проведения доказательства 6.13 необходимы некоторые технические построения и, в частности, один восходящий к Гёделю [8] результат, использующий так называемую *китайскую теорему об остатках*. Наши построения называются *арифметизацией* Σ. Она может быть почти без изменений перенесена на каждую систему Шмульяна. Подобная арифметизация как здесь, так и в других областях является часто используемым вспомогательным средством в вопросах теории вычислимости.

4. Простые арифметические отношения и двучленные функции

Мы определим сначала *числовые выражения* $Z^n(\xi)$ для всех $n \geqslant 0$:

6.15. (a) $Z^0(\xi) := \xi + \xi = \xi$;

(b) $Z^1(\xi) := \xi \times \xi = \xi \wedge \neg Z^0(\xi)$;

(c) $Z^{n+1}(\xi) := \bigvee \eta_1 \bigvee \eta_2 (Z^n(\eta_1) \wedge Z^1(\eta_2) \wedge \xi = \eta_1 + \eta_2)$ $(n \geqslant 1)$.

Предположим при этом, что η_1 и η_2 суть числовые переменные, следующие за ξ. («Следование» понимается в соответствии с упорядочением, индуцированным длинами числовых переменных.)

Мы получаем

6.16. $Z^n(m)$ имеет место тогда и только тогда, когда $m = n$.

При $n = 0$ доказательство тривиально, а при $n \geqslant 1$ проводится индукцией по n. При этом ход рассуждений, в которых используется 6.6, во всем подобен доказательству 6.10 (3).

Далее, имеет место

6.17. Арифметическое выражение $Z^n(\xi)$ содержит по крайней мере n букв.

Определение 6.15 (a)—(c) в действительности является *схемой определений*, так как $Z^n(\xi)$ определено для *каждой* числовой переменной ξ. Договоримся, что во всех нижеследующих схемах определений такого рода с *определяемым* $\alpha(\xi_1, \ldots, \xi_m)$ все входящие в *область определения* и соответствующие числовым переменным (метаязыковые) переменные, если они *различны по написанию*, как и переменные $\xi_1, \ldots, \xi_m$, обозначают *различные* числовые переменные, а именно те числовые переменные, которые по мере их появления непосредственно следуют за наибольшей по длине переменной из ряда $\xi_1, \ldots, \xi_m$.

Пусть

6.18. $Мн(\xi_1, \xi_2) := \bigvee \eta (\neg Z^0(\eta) \wedge \xi_1 + \eta = \xi_2)$.

Мы получаем

6.19. $Мн(n_1, n_2)$ тогда и только тогда, когда $n_1 < n_2$.

Доказательством 6.19 служит следующая цепочка эквивалентных высказываний:

(1) $Мн(\xi_1, \xi_2)$ выполняется при $(\delta^{n_1}_{\xi_1})^{n_2}_{\xi_2}$.

(2) Существует m, для которого $\neg Z^0(\eta) \wedge \xi_1 + \eta = \xi_2$ выполняется при $((\delta^{n_1}_{\xi_1})^{n_2}_{\xi_2})^m_\eta$.

(3) Существует m, $m \neq 0$, такое, что $n_1 + m = n_2$.

(4) $n_1 < n_2$.

Далее мы будем существенно пользоваться *двучленными функциями* σ_2, σ_{21} и σ_{22}: σ_2 взаимно однозначно отображает $\mathbf{N} \times \mathbf{N}$ на $\mathbf{N}$, а σ_{21} и σ_{22} суть обращения σ_2; таким образом,

$$\sigma_2(\sigma_{21}(n), \sigma_{22}(n)) = n,$$
$$\sigma_{2i}(\sigma(n_1, n_2)) = n_i \qquad (i = 1, 2).$$

В отличие от МТВФ II, п. 9 § 3, мы положим здесь

6.20. (a) $\sigma_2(n_1, n_2) := n_1 + \frac{1}{2}(n_1+n_2)(n_1+n_2+1)$;

(b) $\sigma_{21}(n) := n - \frac{1}{2}\left[\sqrt{2n+\frac{1}{4}}-\frac{1}{2}\right]\left(\left[\sqrt{2n+\frac{1}{4}}-\frac{1}{2}\right]+1\right)$;

(c) $\sigma_{22}(n) := \left[\sqrt{2n+\frac{1}{4}}-\frac{1}{2}\right] - \sigma_{21}(n)$.

Здесь через $[\rho]$ обозначена целая часть действительного числа ρ (т. е. наибольшее целое число, не превосходящее ρ).

Если принять во внимание, что $\sigma_2(n_1, n_2) = n_1 + \sum_{i=1}^{n_1+n_2} i$ и что при $\sigma_2(n_1, n_2) = n$ имеет место равенство

$$n_1+n_2 = \sqrt{2n-2n_1+\frac{1}{4}}-\frac{1}{2} = \left[\sqrt{2n+\frac{1}{4}}-\frac{1}{2}\right],$$

то уже нетрудно элементарно обосновать свойства двучленных функций. Далее мы устанавливаем, что $\left[\sqrt{2n+\frac{1}{4}}-\frac{1}{2}\right]$ есть наибольшее натуральное число p, для которого $p^2+p \leqslant 2n$. Это приводит нас к такому определению:

6.21. *Корень* $(\xi_1, \xi_2) := \bigvee\eta_1 \bigvee\eta_2\, (\eta_1 = \xi_1 + \xi_1 \wedge \eta_2 = \xi_2 \times \xi_2 + \xi_2 \wedge \neg\, Мн(\eta_1, \eta_2) \wedge \bigwedge\eta_3 \bigwedge\eta_4\, ((Мн(\xi_2, \eta_3) \wedge \eta_4 = \eta_3 \times \eta_3 + \eta_3) \rightarrow Мн(\eta_1, \eta_4)))$.

Далее получаем такое утверждение:

6.22. *Корень* (n_1, n_2) тогда и только тогда, когда $\left[\sqrt{2n_1+\frac{1}{4}}-\frac{1}{2}\right] = n_2$.

Строгое доказательство этого и последующих подобных утверждений может быть проведено аналогично доказательству 6.19. Мы думаем, что после всех вышеприведенных примеров приемы доказательства стали настолько ясны, что впредь можно отказаться от их подробного проведения. В качестве эвристического вспомогательного средства рекомендуется «содержательное» прочтение определений: вместо $+$ говорить *плюс*, вместо $\neg$ — *не*, вместо *Мн*—*меньше чем*, вместо $Z^n(\xi)$ говорить $\xi = n$ и т. д.

Теперь мы определим схему выражений, которые характеризуют отношения, порожденные уравнениями $\sigma_2(n_1, n_2) = n_3$, $\sigma_{21}(n_1) = n_2$, $\sigma_{22}(n_1) = n_2$:

6.23. (a) $Сигма_2\ (\xi_1, \xi_2, \xi_3) :=$

$$\bigvee \eta_1 \bigvee \eta_2 (Z^1(\eta_1) \wedge \eta_2 + \eta_2 = (\xi_1 + \xi_2) \times (\xi_1 + \xi_2 + \eta_1) \wedge \xi_3 = \\ = \xi_1 + \eta_2).$$

(b) $Сигма_{21}\ (\xi_1, \xi_2) :=$

$$\bigvee \eta_1 \bigvee \eta_2 (Z^1(\eta_1) \wedge Корень(\xi_1, \eta_2) \wedge \xi_2 + \xi_2 + \eta_2 \times (\eta_2 + \eta_1) = \\ = \xi_1 + \xi_1).$$

(c) $Сигма_{22}\ (\xi_1, \xi_2) :=$

$$\bigvee \eta_1 \bigvee \eta_2 (Корень(\xi_1, \eta_1) \wedge Сигма_{21}(\xi_1, \eta_2) \wedge \xi_2 + \eta_2 = \eta_1).$$

Используя 6.20 и 6.22, можно теперь показать, что

6.24. (a) $Сигма_{22}(n_1, n_2, n_3)$ тогда и только тогда, когда $\sigma_2(n_1, n_2) = n_3$;

(b) $Сигма_{21}(n_1, n_2)$ тогда и только тогда, когда $\sigma_{21}(n_1) = n_2$;

(c) $Сигма_{22}(n_1, n_2)$ тогда и только тогда, когда $\sigma_{22}(n_1) = n_2$.

5. Кодирование конечных последовательностей натуральных чисел

В качестве последнего арифметического вспомогательного средства мы рассмотрим кодирование конечных последовательностей натуральных чисел. Каждой такой последовательности $n_0, \ldots, n_{m-1}$ мы сопоставим бесконечное счетное множество натуральных чисел, которые обладают существенным для нас свойством: по каждому из них последовательность $n_0, \ldots, n_{m-1}$ может быть *эффективно* восстановлена. Мы называем эти числа числовыми кодами последовательности $n_0, \ldots, n_{m-1}$.

Введем такое определение:

6.25. Назовем *p числовым кодом* последовательности $n_0, \ldots, n_{m-1}$ тогда и только тогда, когда существует k, для которого

$$p - \sigma_2(\sigma_2(\ldots\sigma_2(\sigma_2(k,\ n_{m-1}),\ n_{m-2})\ldots,\ n_0),\ m).$$

По некоторому числовому коду последовательности $n_0, \ldots, n_{m-1}$ мы можем следующим образом восстановить эту последовательность: сначала $\sigma_{22}(p)$ дает длину последовательности m, а числа $\sigma_{22}(\sigma_{21}^{i+1}(p))$, где $i = 0, \ldots, m-1$, дают нам ряд членов последовательности $n_0, \ldots, n_{m-1}$[1]. Так как значения двучленных функций могут быть вычислены *эффективно*, то и восстановление может быть проведено *эффективно*. Одновременно мы получаем, что каждое число может быть числовым кодом *только одной* конечной последовательности натуральных чисел. В частности, числа вида $\sigma_2(k,\ 0)$ являются числовыми кодами пустой последовательности.

Теперь мы определим двуместные функции f^* и f, отображающие $\mathbf{N}\times\mathbf{N}$ в $\mathbf{N}$:

6.26. (a) $f^*(n_1,\ 0) := \sigma_{21}(n_1)$;
$f^*(n_1,\ n_2+1) := \sigma_{21}(f^*(n_1,\ n_2))$;
(b) $f(n_1,\ n_2) := \sigma_{22}(f^*(n_1,\ n_2))$,

так что $f(n,\ i) = \sigma_{22}(\sigma_{21}^{i+1}(n))$ для $i \geqslant 0$. Если тем не менее p есть числовой код последовательности $n_0, \ldots, n_{m-1}$, то $\sigma_{22}(p)$ определяет длину, а $f(p, i)$ (при $i = 0, \ldots, \sigma_{22}(p) - 1$) — члены (в порядке возрастания индексов) этой последовательности.

В конце этого параграфа мы эффективно определим схему выражений $F^*(\xi_1,\ \xi_2,\ \xi_3)$, для которой

6.27. $F^*(n_1,\ n_2,\ n_3)$ тогда и только тогда, когда $f^*(n_1,\ n_2) = n_3$.

Положив, наконец,

6.28. $F(\xi_1,\ \xi_2,\ \xi_3) := \bigvee\eta\,(F^*(\xi_1,\ \xi_2,\ \eta) \wedge \textit{Сигма}_{22}(\eta)\,\xi_3))$,

получим

6.29. $F(n_1, n_2, n_3)$ тогда и только тогда, когда $f(n_1,\ n_2) = n_3$.

Теперь в нашем распоряжении все вспомогательные средства, нужные для арифметизации Σ, за исключением

[1] Если f — функция, то n-я итерация f определяется так: $f^0 :=$ тождественная функция на Def f, $f^{n+1} = f \circ f^n$ для всех $n \geqslant 0$.

конструкции для $F^*(\xi_1, \xi_2, \xi_3)$. Мы поместили несколько многословное определение $F^*(\xi_1, \xi_2, \xi_3)$ в приложении, чтобы не прерывать надолго ход доказательства.

6. Арифметизация Σ

Система Σ действует над алфавитом A. Пусть $A = \{a_1, \ldots, a_{n_0}\}$. Мы сопоставим взаимно однозначным образом каждому слову над $A \cup \{\rightarrow\}$ (такие слова мы будем называть *псевдословами*) последовательность натуральных чисел, а именно последовательность индексов его букв. При этом индекс буквы $\rightarrow$ мы считаем равным n_0+1. Например, пустому слову отвечает пустая последовательность, слову $a_1a_2a_2$ — последовательность $1, 2, 2$. *Числовыми кодами* псевдослова назовем числовые коды числовой последовательности, сопоставляемой этому слову. Заметим, что каждому псевдослову соответствует бесконечное множество числовых кодов и что

6.30. Из любого числового кода некоторого псевдослова это псевдослово эффективно восстановимо. (Здесь нужно принять во внимание, что из числового кода (числовой) последовательности эта последовательность эффективно восстановима.)

Отношение *быть числовым кодом некоторого псевдослова* может быть арифметизировано. Из определения

6.31. *Псевдослово* $(\xi) := \bigvee \eta_1$ (*Сигма*$_{22}(\xi, \eta_1) \wedge \bigwedge \eta_2$ (*Мн* $(\eta_2, \eta_1) \rightarrow \bigvee \eta_3 (F(\xi, \eta_2, \eta_3) \wedge (Z^1(\eta_3) \vee \ldots \vee Z^{n_0+1}(\eta_3)))))$

мы получаем

6.32. *Псевдослово* (n) тогда и только тогда, когда n есть числовой код некоторого псевдослова.

По поводу *доказательства* заметим, что n есть числовой код псевдослова, когда n есть числовой ход последовательности длины $\sigma_{22}(n)$, члены которой принадлежат множеству $\{1, \ldots, n_0+1\}$.

Слова над A называются в дальнейшем просто *словами*. По аналогии с 6.31 положим

6.33. *Слово* $(\xi) := \bigvee \eta_1$ (*Сигма*$_{22}(\xi, \eta_1) \wedge \bigwedge \eta_2$ (*Мн* $(\eta_2, \eta_1) \rightarrow \rightarrow \bigvee \eta_3 (F(\xi, \eta_2, \eta_3) \wedge (Z^1(\eta_3) \vee \ldots \vee Z^{n_0}(\eta_3)))))$.

Соответственно получим

6.34. *Слово* (n) тогда и только тогда, когда n есть числовой код некоторого слова.

Пусть, далее, $\pi = a_0 \ldots a_{n-1}$ есть псевдослово; для $j = 0, \ldots, n-1$ обозначим через m_j индекс a_j.

Введем определение

6.35. $Код_\pi(\xi) := \bigvee \eta \bigvee \eta_0 \bigvee \eta_0' \ldots \bigvee \eta_{n-1} \bigvee \eta_{n-1}' (Z^n(\eta) \wedge$
$\wedge\, Z^0(\eta_0) \wedge Z^{m_0}(\eta_0') \wedge \ldots \wedge Z^{n-1}(\eta_{n-1}) \wedge Z^{m_{n-1}}(\eta_{n-1}') \wedge$
$\wedge\, Сигма_{22}(\xi, \eta) \wedge F(\xi, \eta_0, \eta_0') \wedge \ldots \wedge F(\xi, \eta_{n-1}, \eta_{n-1}'))$.

Отсюда легко получить следующее утверждение:

6.36. $Код_\pi(n)$ тогда и только тогда, когда n есть числовой код π.

Для ясности заметим, что $Код_\square(\xi) = \bigvee \eta (Z^0(\eta) \wedge$
$\wedge\, Сигма_{22}(\xi, \eta))$.

Наша ближайшая цель—описать при $m \geqslant 2$ конструкцию схемы выражений $Состав_m(\xi_1, \ldots, \xi_{m+1})$, удовлетворяющую следующим требованиям:

6.37. $Состав_m(n_1, \ldots, n_{m+1})$ тогда и только тогда, когда существуют псевдослова $\pi_1, \ldots, \pi_{m+1}$, для которых $\pi_{m+1} =$
$= \pi_1 \ldots \pi_m$ и n_i есть числовой код π_i при $i = 1, \ldots, m+1$.

Обратимся сначала к случаю $m = 2$; для псевдослов π_1 и π_2 имеет место утверждение

6.38. p есть числовой код для π_1, π_2 тогда и только тогда, когда существуют числовые коды p_1 для π_1 и p_2 для π_2, такие, что

(a) $\sigma_{22}(p) = \sigma_{22}(p_1) + \sigma_{22}(p_2)$,
(b) $f(p, i) = f(p_1, i)$ $(0 \leqslant i \leqslant \sigma_{22}(p_1) - 1)$,
(c) $f(p, \sigma_{22}(p_1) + i) = f(p_2, i)$ $(0 \leqslant i \leqslant \sigma_{22}(p_2) - 1)$.

Ввиду этого нужными свойствами обладает следующая схема:

6.39. $Состав_2(\xi_1, \xi_2, \xi_3) :=$
$Псевдослово(\xi_1) \wedge Псевдослово(\xi_2) \wedge Псевдослово(\xi_3) \wedge$
$\wedge \bigvee \eta_1 \bigvee \eta_2 \bigvee \eta_3 (Сигма_{22}(\xi_1, \eta_1) \wedge Сигма_{22}(\xi_2, \eta_2) \wedge Сигма_{22}(\xi_3,$
$\eta_3) \wedge \eta_1 + \eta_2 = \eta_3 \wedge \bigwedge \eta_4 (Мн(\eta_4, \eta_1) \rightarrow \bigvee \eta_5 (F(\xi_1, \eta_4, \eta_5) \wedge$
$\wedge\, F(\xi_3, \eta_4, \eta_5))) \wedge \bigwedge \eta_4 (Мн(\eta_4, \eta_2) \rightarrow \bigvee \eta_5 \bigvee \eta_6 (\eta_1 + \eta_4 =$
$= \eta_6 \vee F(\xi_2, \eta_4, \eta_5) = F(\xi_3, \eta_6, \eta_5))))$.

Состав$_{m+1}(\xi_1, \ldots, \xi_{m+2})$ выражается (при $m \geqslant 2$) через *Состав*$_m(\xi_1, \ldots, \xi_{m+1})$ согласно формуле

6.40. *Состав*$_{m+1}$ $(\xi_1, \ldots, \xi_{m+2})$: $= \bigvee \eta$ (*Состав*$_m$ $(\xi_1, \ldots$ $\ldots, \xi_m, \eta) \wedge$ *Состав*$_2$ $(\eta, \xi_{m+1}, \xi_{m+2}))$.

Теперь мы перейдем к построению схемы выражений *Невывод*(ξ), упомянутой в кратком изложении доказательства; эта схема определяет свойство числа быть числовым кодом некоторого невыводимого в Σ слова (над A). В связи с этим нам необходимо сначала охарактеризовать числовые коды аксиомы $\mathfrak{w}$ системы Σ и числовые коды подстановок и результатов применения правила Modus Ponens. Положим

6.41. *Аксиома* (ξ): $=$ *Код*$_{\mathfrak{w}}(\xi)$.

Ввиду 6.36 мы получаем

6.42. *Аксиома* (n) тогда и только тогда, когда n есть числовой код аксиомы $\mathfrak{w}$ системы Σ.

Пусть $\pi_1, \ldots, \pi_r$ суть неатомарные заключения Σ. Пусть $i \in \{1, \ldots, r\}$ и (ср. 5.8 (b)) $\pi_i = \mathfrak{v}_1\mathfrak{w}_i\mathfrak{v}_2 \to \mathfrak{v}_1\mathfrak{w}'_i\mathfrak{v}_2$. (Случаи, когда отсутствует $\mathfrak{v}_1$ или $\mathfrak{v}_2$, могут быть рассмотрены совершенно аналогично.) Пусть π_1, π_2, π_3 — псевдослова. При этом π_3 есть подстановка π_i с левой частью π_1 и правой частью π_2 тогда и только тогда, когда $\pi_3 = \pi_1 \to \pi_2$ и когда существуют слова w_1, w_2 (над A), для которых $\pi_1 = w_1\mathfrak{w}_i w_2$ и $\pi_2 = w_1\mathfrak{w}'_i w_2$.

Положим

6.43. *Подст*$_i$ (ξ_1, ξ_2, ξ_3): $=$
$\bigvee \eta_1 \bigvee \eta_2 \bigvee \eta_3 \bigvee \eta_4 \bigvee \eta_5$ (*Код*$_{\mathfrak{w}_i}$ $(\eta_1) \wedge$ *Код*$_{\to}$ $(\eta_2) \wedge$ *Код*$_{\mathfrak{w}'_i}$ $(\eta_3) \wedge$
$\wedge$ *Слово* $(\eta_4) \wedge$ *Слово* $(\eta_5) \wedge$ *Состав*$_3$ $(\eta_4, \eta_1, \eta_5, \xi_1) \wedge$
$\wedge$ *Состав*$_3$ $(\eta_4, \eta_3, \eta_5, \xi_2) \wedge$ *Состав*$_3$ $(\xi_1, \eta_2, \xi_2, \xi_3))$.

Получаем

6.44. *Подст*$_i$ (n_1, n_2, n_3) тогда и только тогда, когда существуют псевдослова π_1, π_2, π_3, такие, что n_1, n_2 соответственно n_3 являются числовыми кодами π_1, π_2 соответственно π_3 и $\pi_3 = \pi_1 \to \pi_2$, причем π_3 есть подстановка π_i.

Выводы относительно Σ суть непустые конечные последовательности псевдослов. Всем конечным последовательностям псевдослов мы сопоставляем *числовые коды*: p есть числовой код последовательности псевдослов $\pi_0, \ldots, \pi_{m-1}$

тогда и только тогда, когда существуют числовые коды $p_0, \ldots, p_{m-2}, p_{m-1}$ псевдослов $\pi_0, \ldots, \pi_{m-2}, \pi_{m-1}$ соответственно, такие, что p есть числовой код последовательности $p_0, \ldots, p_{m-1}$. (Последовательность псевдослов обладает бесконечным множеством числовых кодов и по каждому из них последовательность может быть эффективно восстановлена.)

Очевидно, что p есть числовой код вывода относительно Σ тогда и только тогда, когда имеет место следующее:

> p не есть числовой код пустой последовательности (т. е. $\sigma_{22}(p) \neq 0$); каждый член p_i закодированной числом p последовательности чисел есть числовой код псевдослова π_i;
>
> π_i совпадает с аксиомой $\mathfrak{w}$ системы Σ или с подстановкой одного из заключений π_j, либо π_i есть результат применения правила Modus Ponens к псевдословам π_k, π_l, которые соответствуют *предшествующим* p_i членам p_k, p_l. В последнем случае (без ограничения общности) π_k есть подстановка $\alpha \to \beta$ одного из π_j, $\pi_l = \alpha$ и $\pi_i = \beta$.

В связи с этим положим

6.45. $\textit{Вывод}(\xi) := \bigvee \eta_1 (\textit{Сигма}_{22}(\xi, \eta_1) \wedge \neg Z^0(\eta_1) \wedge$
$\wedge \bigwedge \eta_2 \bigwedge \eta_3 ((\textit{Мн}(\eta_2, \eta_1) \wedge F(\xi, \eta_2, \eta_3)) \to (\textit{Аксиома}(\eta_3) \vee$
$\vee \bigvee \eta_4 \bigvee \eta_5 (\textit{Подст}_1(\eta_4, \eta_5, \eta_3) \vee \ldots \vee \textit{Подст}_r(\eta_4, \eta_5, \eta_3)) \vee$
$\vee \bigvee \eta_4 \bigvee \eta_5 \bigvee \eta_6 \bigvee \eta_7 (\textit{Мн}(\eta_4, \eta_2) \wedge \textit{Мн}(\eta_5, \eta_2) \wedge F(\xi, \eta_4, \eta_6) \wedge$
$\wedge F(\xi, \eta_5, \eta_7) \wedge (\textit{Подст}_1(\eta_7, \eta_3, \eta_6) \wedge \ldots \wedge \textit{Подст}_r(\eta_7, \eta_3, \eta_6)))))).$

Получим

6.46. *Вывод* (n) тогда и только тогда, когда n есть числовой код некоторого вывода относительно Σ.

Слово тогда и только тогда невыводимо в Σ, когда оно не является последним членом никакого вывода относительно Σ. Поэтому p является числовым кодом невыводимого относительно Σ слова тогда и только тогда, когда p является числовым кодом некоторого слова и когда для любого q, являющегося числовым кодом некоторого вывода относительно Σ, имеет место неравенство $f(q, \sigma_{22}(q) - 1) \neq p$.

Положим теперь

6.47. *Невывод* $(\xi) := $ *Слово* $(\xi) \wedge$
$\wedge \bigwedge \eta_1 \bigwedge \eta_2 \bigwedge \eta_3 \bigwedge \eta_4$ ((*Вывод* $(\eta_1) \wedge Z^1(\eta_2) \wedge$
$\wedge$ *Сигма*$_{22}(\eta_1, \eta_3) \wedge \eta_4 + \eta_2 = \eta_3) \rightarrow \neg F(\eta_1, \eta_4, \xi))$.

Из вышеизложенных рассуждений следует

6.48. *Невывод* (n) тогда и только тогда, когда n есть числовой код невыводимого в Σ слова.

Теперь мы можем построить арифметическое высказывание α^n, уже упоминавшееся в п. 3:

6.49. $\alpha^n := \bigvee O$ (*Невывод* $(O) \wedge Z^n(O))$ $(n \in \mathbf{N})$.

Имеет место следующее утверждение:

6.50. (a) α^n истинно тогда и только тогда, когда n есть числовой код некоторого *невыводимого* в Σ слова.

(b) α^n состоит не менее чем из n букв.

(В связи с (b) ср. 6.17!)

Мы докажем, кроме того,

6.51. (a) Для данного n α^n может быть задано эффективно.

(b) $\{\alpha^n : n \in \mathbf{N}\}$ разрешимо относительно множества всех арифметических высказываний.

(c) Если $\alpha \in \{\alpha^n : n \in \mathbf{N}\}$, то существует единственное n, для которого $\alpha = \alpha^n$, и это n может быть эффективно вычислено.

Доказательство. (a) следует из того факта, что все составные части высказывания α^n вплоть до схемы выражений $F^*(\xi_1, \xi_2, \xi_3)$ могут быть заданы эффективно. Эффективное построение схемы $F^*(\xi_1, \xi_2, \xi_3)$ дано в приложении.

(b) Мы дадим набросок разрешающей процедуры. Пусть дано арифметическое высказывание α. Сначала устанавливаем число m букв в α. Затем эффективно строим α^0 (это возможно ввиду (a)) и сравниваем α^0 с α. Если $\alpha^0 = \alpha$, то обрываем процедуру, причем с *положительным* результатом. Если $\alpha^0 \neq \alpha$, то эффективно строим α^1 (это возможно ввиду (a)) и поступаем с α^1 так же, как и с α^0, и т. д. Наконец, если $\alpha^m \neq \alpha$, то обрываем процедуру и при этом с *отрицательным* результатом. (Согласно 6.50 (b), $\alpha^k \neq \alpha$ для всех $k \geqslant m + 1$.)

(c) Можно легко показать, что в конъюнкции $(\alpha \wedge \beta)$ арифметические выражения α и β однозначно определены. Далее, согласно 6.16, если $Z^n(\xi) = Z^m(\xi)$, то $n = m$. Если при этом $\alpha^n = \alpha^m$, то (*Невывод* $(O) \wedge Z^n(O)) \equiv$ (*Невывод* $(O) \wedge$ $\wedge Z^m(O))$, так что $n = m$. Наконец, процедура, кратко очерченная в (b), позволяет в том случае, когда $\alpha \in \{\alpha^n : n \in \mathbf{N}\}$, получить число p, для которого $\alpha = \alpha^p$.

Теперь мы в состоянии доказать 6.13 — цель этого параграфа. Предположим, что множество истинных арифметических высказываний перечислимо. Согласно 6.51 (b), мы можем систематическим перечислением этого множества исключить те высказывания, которые не принадлежат множеству $\{\alpha^n : n \in \mathbf{N}\}$. При этом множество истинных арифметических высказываний вида α^n перечислимо. Согласно 6.51 (c), мы можем с помощью перечислительной процедуры для этого множества получить перечислительную процедуру для множества $\{n\colon\ \alpha^n$ истинно$\}$. Вместе с тем, согласно 6.50 (a), множество числовых кодов невыводимых в Σ слов является перечислимым. Так как ввиду 6.30 возможно эффективное восстановление слова по его числовому коду, то, используя те же рассуждения, мы заключаем, что множество невыводимых в Σ слов перечислимо. Это, однако, противоречит 5.8.

Тем самым 6.13 доказано, отсутствует только построение схемы $F^*(\xi_1, \xi_2, \xi_3)$.

7. Приложение. Гёделевский предикат. Схема $F^*(\xi_1, \xi_2, \xi_3)$

В конструкции схемы $F^*(\xi_1, \xi_2, \xi_3)$ мы используем одну восходящую к Гёделю [8] процедуру, в которой применяется так называемая *китайская теорема об остатках*. А именно, функция f^* (ср. 6.26) *определяется индуктивно* с помощью функции σ_{21}, которая уже была описана в 6.23 чисто арифметически: вычисление $f^*(n, m)$ в конце концов сводится к вычислению $f^*(n, 0), \ldots$ $\ldots, f^*(n, m-1)$. Наша ближайшая задача состоит в том, чтобы подходящим способом охарактеризовать такие последовательности чисто арифметически. Для этого мы введем следующую схему выражений, которая определяет так называемый *гёделевский предикат*:

6.52. $G(\xi_1, \xi_2, \xi_3, \xi_4) := \bigvee\eta_1 \bigvee\eta_2 \bigvee\eta_3 (Z^1(\eta_1) \wedge \eta_2 \equiv \eta_1 + (\xi_3 + \eta_1) \times \xi_2 \wedge Мн(\xi_4, \eta_2) \wedge \xi_1 \equiv (\eta_1 + (\xi_3 + \eta_1) \times \xi_2) \times \eta_3 + \xi_4)$.

Очевидно, что $G(n_1, n_2, n_3, n_4)$ выполняется тогда и только тогда, когда $n_4 < 1+(n_3+1)n_2$ и когда существует m, для которого $n_1 = (1+(n_3+1)n_2)m+n_4$, т. е.

6.53. $G(n_1, n_2, n_3, n_4)$ тогда и только тогда, когда n_4 есть остаток от деления n_1 на $1+(n_3+1)n_2$.

Гёделевский предикат обладает следующими важными свойствами:

6.54. (a) Для данных n_1, n_2, n_3 существует *единственное* n_4, для которого $G(n_1, n_2, n_3, n_4)$.

(b) Если $k_0, \ldots, k_m$ есть произвольная (не пустая) конечная последовательность натуральных чисел, то существуют такое n_1 и такое n_2, для которых $G(n_1, n_2, i, k_i)$ имеет место для всех $i \in \{0, \ldots, m\}$.

Доказательство. (a) тривиально, так как $1+(n_3+1)n_2$ всегда больше нуля.

(b) Пусть $k_0, \ldots, k_m$ есть последовательность натуральных чисел длины $m+1$. Положим

$$n_2 := (\max\{m, k_0, \ldots, k_m\})!;$$
$$q_i := 1+(i+1)n_2 \qquad (0 \leqslant i \leqslant m);$$
$$q := \prod_{i=0}^{m} q_i;$$
$$k_i(n) := \text{Остаток от деления } n \text{ на } q_i \ (0 \leqslant n < q,\ 0 \leqslant i \leqslant m).$$

Тогда имеет место утверждение

6.55. (a) Если $0 \leqslant i, j \leqslant m$ и $i \neq j$, то q_i и q_j взаимно просты.

(b) Если $n', n'' < q$ и $n' \neq n''$, то системы остатков $k_0(n'), \ldots, k_m(n')$ и $k_0(n''), \ldots, k_m(n'')$ различны.

Допустим сначала, что 6.55 доказано. Тогда по 6.55 (b) существует q различных систем остатков $k_0(n), \ldots, k_m(n)$. Так как существует ровно q последовательностей длины $m+1$, i-е члены которых меньше q_i для всех $0 \leqslant i \leqslant m$, то каждая такая последовательность является некоторой системой остатков. Так как, далее, для всех членов данной последовательности $k_0, \ldots, k_m$ всегда $k_i \leqslant n_2 < q_i$, то рассматриваемая последовательность также является системой остатков. Поэтому существует такое n_1, $0 \leqslant n_1 < q$, для которого k_i есть остаток n_1 при делении на q_i. Ввиду 6.53 имеем также $G(n_1, n_2, i, k_i)$ для всех i, $0 \leqslant i \leqslant m$.

Осталось доказать 6.55.

(a) Пусть $0 \leqslant i, j \leqslant m$ и p есть простое число, делящее одновременно q_i и q_j. Тогда p делит $q_i - q_j$, а поэтому и $(i-j)n_2$. Так как $q_i \equiv 1 \pmod{n_2}$, то p не может делить n_2, так что p делит число $i-j$. Если бы $i \neq j$, а значит, $0 < |i-j|$, то p делило бы и n_2, так как $|i-j| \leqslant m$, а $m!$ делит n_2. Отсюда следует равенство $i = j$ и тем самым утверждение (a).

(b) Пусть $0 \leqslant n', n'' < q$ и системы остатков $k_0(n'), \ldots$ $\ldots, k_m(n')$ и $k_0(n''), \ldots, k_m(n'')$ совпадают. Тогда каждое q_i делит разность $n' - n''$. Ввиду того что числа q_i попарно взаимно просты (по 6.55(a)), q делит также разность $n' - n''$. Так как $|n' - n''| < q$, то $n' - n'' = 0$, и, таким образом, $n' = n''$, что и требовалось доказать.

Теперь мы положим

6.56. $F^*(\xi_1, \xi_2, \xi_3) := \bigvee \eta_1 \bigvee \eta_2 (\bigvee \eta_3 \bigvee \eta_4 (Z^0(\eta_3) \wedge$
$\wedge\, \mathit{Сигма}_{21}(\xi_1, \eta_4) \wedge G(\eta_1, \eta_2, \eta_3, \eta_4)) \wedge G(\eta_1, \eta_2, \xi_2, \xi_3) \wedge$
$\wedge \bigwedge \eta_3 \bigwedge \eta_4 \bigwedge \eta_5 \bigwedge \eta_6 ((\mathit{Мн}(\eta_3, \xi_2) \wedge \bigvee \eta_7 (Z^1(\eta_7) \wedge \eta_4 \equiv$
$\equiv \eta_3 + \eta_7) \wedge G(\eta_1, \eta_2, \eta_3, \eta_5) \wedge G(\eta_1, \eta_2, \eta_4, \eta_6)) \rightarrow$
$\rightarrow \mathit{Сигма}_{21}(\eta_5, \eta_6)))$.

Тогда для произвольных n_1, n_2, n_3 следующие высказывания эквивалентны:

(1) $F^*(n_1, n_2, n_3)$.

(2) Существуют m_1 и m_2, для которых $G(m_1, m_2, 0, \sigma_{21}(n_1))$ и $G(m_1, m_2, n_2, n_3)$ и для всех m_3, m_4, m_5, m_6, если $m_3 < n_2$ и $m_4 = m_3 + 1$ и $G(m_1, m_2, m_3, m_5)$ и $G(m_1, m_2, m_4, m_6)$, то $m_6 = \sigma_{21}(m_5)$.

(3) Существуют m_1 и m_2, для которых $G(m_1, m_2, 0, \sigma_{21}(n_1))$ и $G(m_1, m_2, n_2, n_3)$ и для всех m_3, m_4, m_5, если $m_3 < n_2$ и $G(m_1, m_2, m_3, m_4)$ и $G(m_1, m_2, m_3 + 1, m_5)$, то $m_5 = \sigma_{21}(m_4)$.

Ввиду 6.54 (a) мы можем продолжить эту цепочку эквивалентных высказываний:

(4) Существуют m_1 и m_2, для которых $G(m_1, m_2, 0, \sigma_{21}(n_1))$ и $G(m_1, m_2, n_2, n_3)$ и для всех m_3, m_4, если $m_3 < n_2$ и $G(m_1, m_2, m_3, m_4)$, то $G(m_1, m_2, m_3+1, \sigma_{21}(m_4))$.

6.27 следует теперь, согласно этой цепочке, из утверждения.

6.57. (4) выполняется тогда и только тогда, когда $f^*(n_1, n_2) = n_3$.

К доказательству 6.57. Предположим сначала, что имеет место (4). Тогда для подходящей пары чисел m_1 и m_2 имеем

(a) $G(m_1, m_2, 0, \sigma_{21}(n_1))$;

(b) $G(m_1, m_2, n_2, n_3)$;

(c) для всех m_3, m_4, если $m_3 < n_2$ и $G(m_1, m_2, m_3, m_4)$, то $G(m_1, m_2, m_3+1, \sigma_{21}(m_4))$.

(a) и (c) дают нам индукцией по m_3

(d) $G(m_1, m_2, m_3, \sigma_{21}^{m_3+1}(n_1))$ для всех $m_3 \leqslant n_2$.

В частности, отсюда следует

(e) $G(m_1, m_2, n_2, \sigma_{21}^{n_2+1}(n_1))$.

Используя (b) и 6.54 (a), получаем далее

(f) $n_3 = \sigma_{21}^{n_2+1}(n_1)$.

Сравнивая (f) с определением f^* (см. 6.26(a)), мы получаем, наконец, нужный нам результат:

(g) $f^*(n_1, n_2) = n_3$.

Обратно, пусть $f^*(n_1, n_2) = n_3$. Рассмотрим последовательность $f^*(n_1, 0)$, $f^*(n_1, 1)$, ..., $f^*(n_1, n_2)$. Согласно 6.54 (b), существуют числа m_1 и m_2, для которых

$$G(m_1, m_2, i, f^*(n_1, i)) \text{ для всех } i,\ 0 \leqslant i \leqslant n_2.$$

Так как $f^*(n_1, i+1) = \sigma_{21}(f^*(n_1, i))$ при $i \geqslant 0$, существуют числа m_1 и m_2 со следующими свойствами:

$G(m_1, m_2, 0, f^*(n_1, 0))$,

$G(m_1, m_2, n_2, f^*(n_1, n_2))$ и

для всех m_3, m_4, если $m_3 < n_2$ и $G(m_1, m_2, m_3, m_4)$, то $G(m_1, m_2, m_3+1, \sigma_{21}(m_4))$.

Заметив, что $f^*(n_1, 0) = \sigma_{21}(n_1)$ и что $f^*(n_1, n_2) = n_3$, мы получим (4).

ЛИТЕРАТУРА

1. Brauer W., Indermark K., Algorithmen, rekursive Funktionen und formale Sprachen, Mannheim — Zürich, Bibliographisches Institut, 1969.
2. Хомский Н., Формальные свойства грамматик, Кибернетический сб., вып. 2, «Мир», М., 1966.
3. Хомский Н., Миллер Г. А., Введение в формальный анализ естественных языков, Кибернетический сб., вып. 1, «Мир», М., 1965.
4. Church A., A Note on the Entscheidungsproblem, *J. Symb. Logic*, 1 (1936), 40—41; 101—102.
5. Davis M., Computability and Unsolvability, New York — Toronto — London, McGraw-Hill, 1958.
6. Gerhardt C. I., Die philosophischen Schriften von Gottfried Wilhelm Leibnitz, Vol. I, Berlin, 1875.
7. Gödel K., Die Vollständigkeit der Axiome des logischen Funktionenkalküls, *Monatsh. Math. Phys.*, 37 (1930), 349—360.
8. Gödel K., Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I, Ibid, 38 (1931), 173—198.
9. Hermes H., Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit, Berlin — Göttingen — Heidelberg, Springer, 1961.
10. Kleene S. C., Recursive Predicates and Quantifiers, *Trans. Amer. Math. Soc.*, 53 (1943), 41—73.
11. Lorenzen P., Einführung in die operative Logik und Mathematik, Berlin — Göttingen — Heidelberg, Springer, 1955.
12. Post E. L., Formal Reductions of the General Combinatorial Decision Problem, *Amer. J. Math.*, 65 (1943), 197—215.
13. Post E. L., Recursively Enumerable Sets of Positive Integers and Their Decision Problems, *Bull. Amer. Math. Soc.*, 50 (1944), 284—316.
14. Rogers H., Theory of Recursive Functions and Effective Computability, New York — St. Louis, McGraw-Hill, 1967.
15. Smullyan R. M., Theory of Formal Systems, Princeton, 1961; 2 ed., Princeton, Princeton Univ. Press., 1968.
16. Tarski A., Der Wahrheitsbegriff in den formalisierten Sprachen, *Studia Philosophica*, 1 (1936), 261—405.
17. Tarski A., Mostowski A., Robinson R. M., Undecidable Theories, Amsterdam, North-Holland Publishing Co., 1953.

18*. Бурбаки Н., Очерки по истории математики, ИЛ, М., 1963.

19*. Кроуэлл Р., Фокс Р., Введение в теорию узлов, «Мир», М., 1967.

ПРОБЛЕМА РАЗРЕШИМОСТИ И ИГРА «ДОМИНО»

Г. ХЕРМЕС

Проблема разрешимости логики предикатов состоит в следующем: существует ли процедура, с помощью которой для каждого выражения из класса выражений (формул), заданных префиксом их предваренной нормальной формы, можно решить, выполнимо оно или нет. Этот вопрос для классов, определенных префиксом $\bigwedge\bigvee\bigwedge$, долго оставался открытым. Ответ (отрицательный) был впервые получен в 1962 г. При этом была обнаружена связь с машинами Тьюринга, возникающая при рассмотрении так называемых игр «домино». В этой статье мы хотим (1) дать обзор некоторых результатов по проблеме разрешимости логики предикатов, (2) сформулировать различные принадлежащие Вану определения игр «домино», (3) для некоторого неполного варианта $\bigwedge\bigvee\bigwedge$-случая провести доказательства неразрешимости с помощью игры «домино». Этот результат принадлежит Бюхи; полностью $\bigwedge\bigvee\bigwedge$-случай был рассмотрен Каром, Муром и Ваном.

§ 1. *К проблеме разрешимости логики предикатов. Часть 1*

В течение последних ста лет были созданы различные формальные языки. Одним из них является *логика предикатов первой ступени*. Существует несколько вариантов этого языка, различающихся между собой своими выразительными возможностями. Если не допускаются ни функциональные символы, ни равенство, то говорят об *узкой логике предикатов первой ступени*. Наряду с узкой логикой предикатов здесь будет играть роль язык, в котором допускаются функциональные символы, но не допускается знак равенства. О построении этих языков см. § 2.

Выражения—это последовательности символов, образуемые по правилам языка логики предикатов (см. § 2).

Для логики особенно важно свойство *выполнимости* выражений (ср. § 3). Можно интересоваться вопросом разрешимости этого свойства (по поводу понятий разрешимости, перечислимости, машин Тьюринга и т. п. см. предыдущие статьи о машинах Тьюринга и перечислимости).

Рассмотрим логическое исчисление. Оно состоит из системы правил для получения выражений. Выражения, получаемые с помощью этих правил, называются *выводимыми*. Для каждого выражения α справедливо утверждение: α невыводимо тогда и только тогда, когда выводимо $\neg\alpha$ (т. е. отрицание α). Это показывает, что множество невыводимых высказываний перечислимо.

Вопрос о том, является ли выполнимость сама по себе разрешимым свойством, долго оставался открытым. Чтобы прийти к каким-то результатам, ограничиваются рассмотрением выражений из определенных классов выражений. Можно показать, что для некоторых таких классов выполнимость есть разрешимое свойство. (В связи с этим см. довольно полное изложение у Аккермана [8].)

Для других классов выражений $\mathfrak{A}$ было показано, что они являются так называемыми *редукционными классами*. Это означает, что разрешимость свойства выполнимости *произвольных* выражений узкой логики предикатов первой ступени может быть сведена в следующем смысле к разрешимости свойства выполнимости выражений из $\mathfrak{A}$: каждому выражению β узкой логики предикатов может быть эффективным образом сопоставлено выражение α из $\mathfrak{A}$, которое выполнимо в том и только том случае, когда выполнимо β. Таким образом, если свойство выполнимости может быть разрешено в $\mathfrak{A}$, то оно может быть разрешено и для произвольных выражений из узкой логики предикатов.

В 1936 г. Чёрч показал, что выполнимость выражений узкой логики предикатов есть неразрешимое свойство («Неразрешимость проблемы разрешимости для узкой логики предикатов»[1])). Отсюда следует, что свойство выпол-

[1]) Точнее, «Проблема разрешимости для узкой логики предикатов не имеет положительного решения». Противоречивая тавтологичность русского оборота: «неразрешимость ... разрешимости» устраняется в немецком языке: «Unlösbarkeit des Entscheidungsproblems». — *Прим. перев.*

нимости является неразрешимым и для каждого редукционного класса.

Используя теорию машин Тьюринга, можно дать следующий набросок доказательства неразрешимости проблемы разрешимости узкой логики предикатов. Каждой таблице Тьюринга T эффективным образом сопоставляется некоторое выражение φ_T узкой логики предикатов, с тем чтобы имела место следующая эквивалентность:

(1.1) $M(T)$ останавливается после применения к пустой ленте через конечное число шагов тогда и только тогда, когда φ_T невыполнимо.

В результате такого соответствия из разрешимости свойства выполнимости выражений вытекает разрешимость *проблемы останова*, т. е. свойства $M(T)$ останавливаться после применения к пустой ленте через конечное число шагов. Но для этого не существует никакой разрешающей процедуры (ср. статью о машинах Тьюринга, § 5).

Могло бы случиться, что для каждой машины T выражение φ_T лежит в заданном классе выражений $\mathfrak{A}$. Очевидно, что тогда проблема разрешимости для $\mathfrak{A}$ также не имеет решения. *Более того, $\mathfrak{A}$ является даже редукционным классом.* Это можно установить следующим образом: мы уже заметили, что α невыполнимо тогда и только тогда, когда $\neg\alpha$ выводимо; поэтому можно построить такую таблицу Тьюринга T_0, чтобы $M(T_0)$ останавливалась после применения к отрицанию $\neg\alpha$ произвольного выражения α через конечное число шагов в том и только в том случае, когда α невыполнимо (ср. теорему 3.6 предшествующей статьи о перечислимости). Пусть теперь T_0^α есть таблица Тьюринга, такая, что $M(T_0^\alpha)$, примененная к пустой ленте, сначала пишет на ней $\neg\alpha$, а дальше работает как T_0, примененная к $\neg\alpha$. Мы получаем таким образом

(1.2) $M(T_0^\alpha)$ останавливается после применения к пустой ленте через конечное число шагов тогда и только тогда, когда α невыполнимо.

Из (1.1) и (1.2) непосредственно следует

(1.3) α выполнимо тогда и только тогда, когда выполнимо $\varphi_{T_0^\alpha}$.

Согласно нашему предположению, $\varphi_{T_0\alpha}$ принадлежит классу выражений $\mathfrak{A}$. Исходя из α, можно сначала эффективно получить T_0^{α}, а затем и $\varphi_{T_0\alpha}$. Тем самым показано, что $\mathfrak{A}$ есть редукционный класс.

Исчерпывающее изложенне вопросов, связанных с редукционными классами, можно найти в книге Сураньи [9].

В связи с проблемой разрешимости наибольший интерес представляют прежде всего такие классы выражений, которые могут быть охарактеризованы типом префиксов (ср. § 2). Об этом мы рассказываем в § 4, излагая сначала в § 2 и 3 ряд определений.

§ 2. *Выражения, префиксы, типы префиксов. Классы выражений, определяемые такими типами*

Здесь и далее в § 3 мы максимально кратко н по возможности на примерах дадим несколько основных определений логики предикатов. Исчерпывающее изложение можно найти, например, в книге Хермеса [6] [1]) (см. также § 6 предыдущей статьи о перечислимости). Хотя здесь нас интересует в конечном счете лишь узкая логика предикатов, мы будем рассматривать и функциональные символы, так как в одном из доказательств в качестве промежуточиого шага возникает выражение, содержащее функциональный символ (§ 9).

Мы исходим из счетного множества *индивидных символов* [2]), счетного множества *предикатных символов* всех порядков $k \geqslant 1$ и счетного множества *функциональных символов* всех порядков $k \geqslant 1$ [3]). Индивидные символы мы обозначаем буквами x, y, x_1, x_2, ..., предикатные символы — буквами $P, Q, A, B, \ldots$, функциональные символы — буквами f, g, ... Из индивидных символов и функциональных символов в соответствии с их порядком можно образовывать *термы*. Примеры термов: x, fx, $gfxy$ (с одно-

[1]) Или Чёрча [10]. — *Прим. перев.*

[2]) В предыдущей статье онн назывались символами переменных. — *Прим. перев.*

[3]) Предикатный (функциональный) снмвол k-го порядка называется также k-местным предикатным (функцнональным) символом. — *Прим. перев.*

местным f и двуместным g; в последием примере fx является первым аргументом g). В качестве обозначеиий для термов мы используем буквы t, t_1, t_2, ... Если P есть k-местный предикат, то $Pt_1 \dots t_k$ есть *атомарное выражение*. Из атомарных выражений можно строить *сложные выражения* с применением скобок и связок $\neg$ (не), $\wedge$ (и), $\vee$ (или), $\rightarrow$ (если, то), а также кванторов $\bigwedge$ (для всех) и $\bigvee$ (существует). Примеры выражений (с одноместным P и двуместным Q):

$$Px,\quad Pfx,\quad Qxy,\quad \neg Px,\quad \bigwedge x(Px \rightarrow (\neg Pfx \vee Qxy)),$$
$$\neg(\bigvee xPx \wedge \neg Pfx),\ \neg \bigvee x(Px \wedge \neg Pfx),\quad \bigwedge y \bigwedge zQzy.$$

В качестве обозиачений для выражений мы используем буквы α, β, ...

Каждый ннднвидиый символ, иаходящийся в выражении иа определеином месте, входит туда свободиым или связанным образом. Например, символ x в выражении $(Px \wedge \bigwedge xPfx)$ имеет свободное вхождение в первое из мест, где он встречается, и связанное (квантором $\bigwedge$) в двух последующих. Выражение, в которое ни один из символов ие входит ни в какое из мест свободно, иазывается *замкнутым*. Примеры: $\bigwedge xPx$, $\bigvee y \bigwedge xQxy$.

Свободные индивидиые символы, символы предикатов и функциональные символы называются *переменными* α; $V(\alpha)$ есть множество переменных α. Например, имеем $V((\bigwedge xQy \vee \bigvee zQxfz)) = \{x,\ y,\ Q,\ f\}$ (x и y — различные символы). Выражение α замкнуто тогда и только тогда, когда среди элементов $V(\alpha)$ нет индивидных переменных. Мы называем *α выражением узкой логики предикатов*, когда среди элементов $V(\alpha)$ нет функциональных символов.

Последовательности символов вида $Q_1x_1 \dots Q_rx_r$, где каждый из символов Q_i есть один из двух кванторов $\bigwedge$, $\bigvee$, называются *префиксами*. Пустая последовательность символов также называется префиксом. Примеры префиксов: $\bigwedge x \bigvee y \bigwedge z$, $\bigvee x \bigvee x$. Если мы опустим в префиксе входящие в него иидивидиые символы, то мы получим *тип* префнкса. Рассмотренные выше в качестве примеров префиксы имеют типы $\bigwedge\bigvee\bigwedge$, $\bigvee\bigvee$. Для краткости мы будем, например, вместо $\bigwedge\bigwedge\bigvee\bigvee\bigwedge\bigwedge\bigwedge$ писать $\bigwedge^2\bigvee^2\bigwedge^3$. В качестве обозначеиий для префиксов мы пользуемся буквами $\Pi, \Pi_1, \Pi_2, \dots$, для типов префиксов—буквами $\pi, \pi_1, \pi_2, \dots$.

В классе типов префиксов можно ввести *частичное упорядочение*, считая, что $\pi_1 \leqslant \pi_2$ в том и только в том случае, когда π_2 может быть получено из π_1 введением дополнительных кванторов в подходящих местах π_1. Например, верно, что $\bigwedge\bigvee\bigwedge \leqslant \bigvee^2\bigwedge\bigvee^2\bigwedge^3\bigvee$, но неверно, что $\bigwedge\bigvee\bigwedge \leqslant \bigvee\bigwedge\bigvee$. Нетрудно проверить, что имеет место

2.1. Лемма. *Для каждого типа префиксов π имеет место один из следующих случаев*:

(1) $\bigwedge\bigvee\bigwedge \leqslant \pi$;

(2) $\bigwedge^3\bigvee \leqslant \pi$;

(3) $\pi \leqslant \bigvee^r\bigvee^s$ (по крайней мере для одной пары чисел $r \geqslant 0$, $s \geqslant 0$);

(4) $\pi \leqslant \bigvee^r\bigwedge^2\bigvee^s$ (по крайней мере для одной пары чисел $r \geqslant 0$, $s \geqslant 0$).

Будем говорить, что выражение α имеет вид *предваренной нормальной формы*, если оно имеет внд $\Pi\beta$, где β есть выражение без кванторов. Примеры предваренных нормальных форм: $\bigwedge x\,Qxy$, $\bigvee y\bigwedge x\,Qxy$, $\bigwedge z\bigvee x\,(Px \rightarrow Qxy)$, Qxy. Выражение $\bigwedge z\,(\bigvee x\,Px \rightarrow Qxy)$ не является предваренной нормальной формой (ввиду наличия скобки на третьем месте).

Типу π префиксов можно однозначно сопоставить класс $\mathfrak{A}(\pi)$ всех замкнутых предваренных выражений узкой логики предикатов, тип префикса которых есть π. Вместо $\mathfrak{A}(\pi)$ мы будем кратко писать π, когда из контекста ясно, о чем идет речь. К классу выражений $\bigwedge\bigvee$ принадлежат, например, выражения $\bigwedge x \bigvee xPx$, $\bigwedge x \bigvee y\,(Qxy \rightarrow Px)$.

§ 3. *Выполнимость выражений* [1])

Под интерпретацией $\mathfrak{I}$ мы понимаем упорядоченную пару $\langle B, I\rangle$ со следующими свойствами:

(1) B есть непустое множество (называемое в этой связи *областью индивидов*).

(2) I есть отображение, которое определено для неко-

[1]) Материал этого параграфа перекликается с некоторыми разделами книги Р. Линдона [11].— *Прим. перев.*

торых индивидных символов, символов предикатов и функциональных символов. При этом:

(2.1) Если $I(x)$ определено, то $I(x) \in B$.

(2.2) Если $I(P)$ определено, то $I(P)$ есть отношение между элементами B, порядок которого совпадает с порядком P.

(2.3) Если $I(f)$ определено и f есть k-местная функция, то $I(f)$ есть отображение B^k в B.

$\mathfrak{I} = \langle B, I \rangle$ называется *интерпретацией* α, если I определено для каждого параметра $V(\alpha)$. Посредством такой интерпретации $\mathfrak{I}$ переменным α сопоставляется некоторое значение. При этом имеет смысл говорить, что α *выполнимо в интерпретации* $\mathfrak{I}$. Это основополагающее отношение может быть определено рекурсивно при конструировании выражений. Мы не станем здесь давать такое определение и ограничимся примерами. (Точное определение для «арифметического языка» можно найти в п. 2 § 6 предыдущей статьи о перечислимости.) Предположим, что B есть множество натуральных чисел. Пусть I определено для x, y, P, Q и f. Пусть $I(x) = 0$, $I(y) = 2$, $I(P)$ есть свойство быть простым числом, $I(Q)$ есть отношение меньше чем и $I(f)$ есть квадратная функция. Положим $\mathfrak{I} = \langle B, I \rangle$. Тогда мы имеем для $\mathfrak{I}$ (при этом предполагается, что x, y, z суть различные субъектные символы):

(a) Py выполнимо (так как 2 — простое число),

(b) Px невыполнимо (так как 0 не есть простое число),

(c) $\neg P(x)$ выполнимо (так как $P(x)$ невыполнимо),

(d) $(Py \wedge \neg Px)$ выполнимо (ввиду (a) и (c)),

(e) $\bigwedge z\,(Pz \rightarrow Qxz)$ выполнимо (так как каждое простое число больше 0),

(f) $\bigwedge y\,(Py \rightarrow Qxy)$ выполнимо (это означает то же, что и (e); y связано здесь квантором $\bigwedge$, поэтому $I(y)$ ни на что не влияет),

(g) $\bigvee x\,Pfx$ невыполнимо (так как квадрат не может быть простым числом),

(h) $\bigwedge x \bigvee y\,Qxy$ выполнимо (так как для каждого натурального числа найдется большее).

Выражение α называется *выполнимым*, если существует интерпретация α, в которой α выполнимо. Примеры можно найти в вышеприведенном списке. $\bigvee x\,Pfx$ невыполнимо в вышеописанной интерпретации. Тем не менее $\bigvee x\,Pfx$

выполнимо (подыщите для этого подходящую интерпретацию!). $(Px \wedge \neg Px)$ невыполнимо.

Выполнимость является основополагающим логическим понятием, с которым связан целый ряд дальнейших существенных понятий. Так, например, *выражение* β *следует из выражения* α, если выражение $(\alpha \wedge \neg \beta)$ невыполнимо.

Два выражения α и β называются *эквивалентными*, если в каждой интерпретации $\mathfrak{J}$ обоих этих выражений они либо одновременно выполняются, либо одновременно не выполняются. Эквивалентные выражения α, β являются *равновыполнимыми*, т. е. α выполняется тогда и только тогда, когда выполняется β.

Для каждого выражения α можно подыскать некоторое равновыполнимое выражение β из *узкой* логики предикатов. Это можно проделать, используя *метод Сколема* исключения функциональных символов. Один характерный пример обсуждается в § 11.

Каждому выражению α узкой логики предикатов можно эффективно сопоставить эквивалентное выражение β узкой логики предикатов, которое имеет предваренную нормальную форму. Так, например, $(\bigwedge x Px \vee Py)$ эквивалентно $\bigwedge x (Px \vee Py)$, а $(\bigwedge x Px \rightarrow Py)$ эквивалентно $\bigvee x (Px \rightarrow Py)$ (x, y — разные субъектные символы).

Для каждого выражения α можно построить равновыполнимое замкнутое выражение β, написав перед α префикс типа $\bigvee^r$, в который включены свободно входящие в α индивидные символы. Так, $(\bigwedge x Qxy \rightarrow Pz)$ равновыполнимо с $\bigvee y \bigvee z (\bigwedge x Qxy \rightarrow Pz)$ (x, y, z попарно различны).

Три последних замечания показывают, что при обсуждении вопроса о разрешимости можно ограничиться замкнутыми высказываниями узкой логики в предваренной форме.

3.1. Лемма. *Пусть* $\pi_1 \leqslant \pi_2$ (ср. § 2). *Тогда можно каждому выражению* $\alpha_1 \in \pi_1$ (*по поводу этого обозначения см. конец* § 2) *эффективно сопоставить эквивалентное* (*а значит, и равновыполнимое*) *выражение* $\alpha_2 \in \pi_2$.

Доказательство. Выражение нужного вида получится, если дополнить префикс в α_1, применяемый к субъектным символам, не входящим в α_2, таким образом, чтобы получить префикс типа π_2. Эквивалентность α_1 и α_2 следует из транзитивности эквивалентности и из двух следующих элементарных фактов:

(1) Если x не входит в α, то α эквивалентно $\bigwedge x\alpha$ и $\bigvee x\alpha$.

(2) Если α эквивалентно β, то $\bigwedge x\alpha$ эквивалентно $\bigwedge x\beta$ и $\bigvee x\alpha$ эквивалентно $\bigvee x\beta$.

§ 4. *К проблеме разрешимости логики предикатов. Часть 2*

Здесь нужно упомянуть о нескольких результатах, относящихся к классам выражений π, характеризуемых своими префиксами (ср. конец § 2).

а) *Решения проблем разрешимости.* В 1928 г. Бернайс и Шёнфинкель показали, что проблема разрешимости для всех классов выражений $\bigvee^r \bigwedge^s$ $(r \geqslant 0,\ s \geqslant 0)$ (см. (3) в лемме 2.1) решается положительно; таким образом, существует алгоритм, с помощью которого для каждого выражения α из любого такого класса можно за конечное число шагов установить, выполнимо это выражение или нет. Независимо друг от друга Гёдель, Кальмар и Шютте в 1932—1934 гг. показали, что проблема разрешимости имеет положительное решение и для классов выражений $\bigvee^r \bigwedge^2 \bigvee^s$ $(r \geqslant 0,\ s \geqslant 0)$ (см. (4) в *лемме* 2.1).

b) *Редукции проблемы разрешимости.* Сколем уже в 1920 г. показал, что объединение всех классов выражений $\bigwedge^r \bigvee^s$ $(r \geqslant 0, s \geqslant 0)$ есть некоторый редукционный класс (т. е. что для каждого выражения узкой логики предикатов может быть эффективно построено равновыполнимое выражение, лежащее в одном из классов $\bigwedge^r \bigvee^s$). Этот результат был усилен Гёделем (1933) и позже Сураньи (1943). Сураньи показал, что уже $\bigwedge^3 \bigvee$ есть редукционный класс (ср. (2) в лемме 2.1). Только после появления упоминавшейся в § 1 книги Сураньи стал известен в некотором смысле окончательный результат. В 1962 г. Кар, Мур и Ван показали, что $\bigwedge \bigvee \bigwedge$ есть редукционный класс (см. (1) в лемме 2.1). Мы получаем тем самым следующую теорему:

4.1. Теорема. *Класс выражений π (т. е. класс замкнутых предваренных выражений узкой логики предикатов, префикс которых принадлежит к типу π) неразрешим тогда и только тогда (и является даже редукционным* *классом), когда* $\wedge\vee\wedge \leqslant \pi$ *или когда* $\wedge^3\vee \leqslant \pi$. *(Естественно, что для каждого* π *разрешимо, какой из этих двух типов имеет место.)*

Доказательство. (a) Если $\wedge\vee\wedge \leqslant \pi$ или $\wedge^3\vee \leqslant \pi$, то по лемме 3.1 для каждого выражения $\alpha \in \wedge\vee\wedge$, соответственно $\alpha \in \wedge^3\vee$, можно эффективным образом подыскать равновыполнимое выражение из π. Так как $\wedge\vee\wedge$ и $\vee^3\vee$ — редукциоиные классы, то π — тоже редукционный класс.

(b) Если не выполнено ни $\wedge\vee\wedge \leqslant \pi$, ни $\wedge^3\vee \leqslant \pi$, то по лемме 2.1 имеем $\pi \leqslant \vee^r\wedge^s$ или $\pi \leqslant \vee^r\wedge^2\vee^s$ для некоторых r, s. Тогда по лемме 3.1 для каждого выражеиия $\alpha \in \pi$ можно эффективиым образом найти равновыполнимое выражение из $\vee^r\wedge^s$, соответственно из $\vee^r\wedge^2\vee^s$. Однако для этих классов выражений проблема разрешимости имеет положительное решеиие. Тем самым может быть также разрешено, выполнимо или иет выражеиие α.

В доказательстве теоремы Кара, Мура и Вана применяется описанная в § 1 процедура эффективного сопоставления каждой таблице Тьюринга T формулы φ_T, для которой имеет место (1.1). Конструкция φ_T получается на обходном пути в связн с изучением «проблемы домино». Есть несколько вариаитов проблемы домино: «угловая проблема», «диагоиальная проблема» и «общая проблема». Точную формулировку можио найти в § 5. Ваи [1] показал, что угловая проблема неразрешима. Удачно применив метод Сколема исключения функциоиальных символов, Бюхи [2, 3] показал, что из неразрешимости угловой проблемы следует, что класс выражений $\vee \wedge \wedge\vee\wedge$ является редукционным классом. ($\vee \wedge \wedge\vee\wedge$ есть коиъюикция выражения из класса $\vee$ и выражения нз класса $\wedge\vee\wedge$.) Кар, Мур и Ван показали в [4], что диагональная проблема также неразрешима, и, используя метод Бюхи, устаиовили, что $\wedge\vee\wedge$ есть редукционный класс. Неразрешимость общей проблемы домино была показана в [5] Бергером.

Замечание. В центре иашего внимания было *свойство выполнимости*, и мы пришли таким образом *к проблеме разрешимости в связи с выполнимостью*. Можно было бы исходить из свойства *универсальной выполнимости*. Выражение называется универсально выполнимым, если оно выполнимо в любой интерпретации. Понятия выполнимости и универсальной выполнимости тесно связаны между собой, что видно из легко проверяемой теоремы:

Теорема. (1) *α выполнимо тогда и только тогда, когда $\neg\alpha$ не универсально выполнимо.*

(2) *α универсально выполнимо тогда и только тогда, когда $\neg\alpha$ невыполнимо.*

Отсюда сразу следует, что проблема разрешимости для универсальной выполнимости неразрешима. Отметим далее, что $\neg\Pi\alpha$ эквивалентно $\Pi^{-1}\neg\alpha$, где префикс Π^{-1} получается из префикса Π заменой кванторов $\bigwedge$ кванторами $\bigvee$, и наоборот; таким образом, из теоремы 4.1 можно получить аналог для универсальной выполнимости. В литературе по проблеме разрешимости понятие выполнимости предшествует понятию универсальной выполнимости.

Дальнейшие разделы этой статьи содержат:

(1) формулировку различных проблем домино (§ 5),

(2) доказательство неразрешимости угловой проблемы (§ 6, 7, 8),

(3) доказательство того факта, что $\bigvee\wedge\bigwedge\bigvee\bigwedge$ есть редукционный класс (§ 9, 10, 12),

(4) замечания по поводу доказательства неразрешимости диагональной проблемы и того факта, что $\bigwedge\bigvee\bigwedge$ есть редукционный класс (§ 13).

§ 5. Проблемы домино

(Для понимания этого параграфа не нужны никакие предварительные знания.) *Домино*—это квадратная пластинка[1]) со стороной 1 следующего вида:

(1) Пластинка имеет *верхнюю* и *нижнюю* поверхности.

(2) Нижняя поверхность не обладает никакими особенными признаками.

(3) Края (стороны) верхней поверхности называются (в порядке, соответствующем обходу пластинки по часовой стрелке, если смотреть сверху) *верхним*, *правым*, *нижним* и *левым краем*.

(4) Каждый край верхней поверхности раскрашен в свой цвет.

[1]) В русском языке слово *домино* употребляют как название игры, в которой используются *кости* домино.—*Прим. перев.*

(Одно домнно может быть раскрашено не более чем в четыре различных цвета, но может встречаться и меньшее число цветов.) Цвет верхнего края называется *верхним* и т. д. В дальнейшем домино представляются в том виде, в каком они изображены на рис. 1. При этом у изображенного там домино (A) верхний цвет — зеленый, правый — желтый, нижний — красный, а левый — голубой.

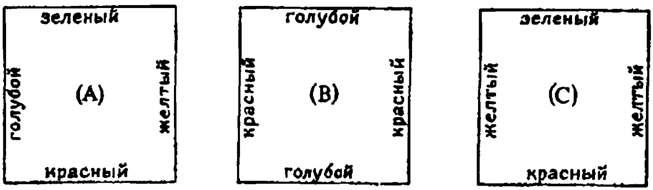


Рис. 1. Примеры домнно.

Два домино называются *эквивалентными*, если их соответственные стороны окрашены в одинаковые цвета. Эквивалентные домино принадлежат к одному *типу домино*. В дальнейшем мы, вообще говоря, не будем на словах проводить различие между домино и типами домино, так как из контекста всегда будет ясно, что имеется в виду.

Типам домино и домино одинаковых типов можно присваивать *имена*. Удобно представлять себе домино с именами, вписанными в середину верхией поверхности домино, как на рис. 1.

Общая игра «домино» задается непустым конечным множеством $\mathfrak{D}$ типов домино. Предположим, что на плоскости задана сетка, образованная прямыми, параллельными координатным осям и проходящими через целочисленные точки на осях. Мы получим *покрытие* посредством $\mathfrak{D}$, если в каждый квадрат сетки положим домино, принадлежащее одному из типов множества $\mathfrak{D}$. Покрытие посредством $\mathfrak{D}$ называется *когерентным*, если все домино соприкасаются по сторонам, окрашенным в один цвет. Игра «домино» $\mathfrak{D}$ называется *правильной*, еслн существует когерентное покрытие посредством $\mathfrak{D}$.

Если $\mathfrak{D}$ содержит тип (B) (ср. рис. 1), то мы получим когерентное покрытие, положив на каждый квадрат домино (B). Итак, $\mathfrak{D}$ правнльна. Это покрытие тривиальным образом является «периодическим». Имеются примеры правильных игр «домино», для которых не существует периодических когерентиых покрытий.

Если $\mathfrak{D}$ состоит только из типов (A) и (C) (ср. рис. 1), то ие существует иикакого когереитного покрытия посредством $\mathfrak{D}$ (так как зеленый цвет является верхинм цветом каждого домино из $\mathfrak{D}$ и не является нижним цветом ни одного из них). Таким образом, $\mathfrak{D}$ неправильна.

Угловая игра «домино» задается конечным множеством $\mathfrak{D}$ типов домино и иепустым подмиожеством $\mathfrak{D}^0 \subset \mathfrak{D}$. *Угловое покрытие посредством* $\mathfrak{D}$, $\mathfrak{D}^0$ можно получить, если в каждый квадрат *первого квадранта* положить домино одного из типов $\mathfrak{D}$ и, в частности, в *угловой квадрат* положить домино одиого из типов $\mathfrak{D}^0$. *Когерентность* углового покрытия определяется так же, как и в общей игре *«домино»*, $\mathfrak{D}$, $\mathfrak{D}^0$ называется *правильной* парой, если существует когерентное угловое покрытие посредством $\mathfrak{D}$, $\mathfrak{D}^0$.

Диагональная игра «домино» определяется, как и угловая игра «домино», парой миожеств $\mathfrak{D}$, $\mathfrak{D}^0$. *Диагональное покрытие* посредством $\mathfrak{D}$, $\mathfrak{D}^0$ можно получить, положив на каждый квадрат первого квадранта домиио, принадлежащее одному из типов $\mathfrak{D}$, и, в частности, на каждый квадрат, лежащий на *диагонали* первого квадранта, домиио, прииадлежащее одному из типов $\mathfrak{D}^0$. *Когерентность* диагоиального покрытия определяется так же, как и в общей игре «домино». $\mathfrak{D}$, $\mathfrak{D}_0$ называется *правильной* парой, если существует когерентное диагональное покрытие посредством $\mathfrak{D}$, $\mathfrak{D}_0$.

В отдельных случаях удается установить, является ли коикретная общая (угловая, диагональиая) игра «домино» правильной. Можно задаться вопросом, имеется ли алгоритм, с помощью которого для всякой такой игры за конечное число шагов можно установить, правильная она или нет. На этот вопрос приходится ответить отрицательио.

5.1. Теорема (*неразрешимость проблемы домино*). *Определенное для угловой игры «домино» свойство быть правильной неразрешимо* (Ван, 1961). *То же имеет место для диагональной игры «домино»* (Кар, Мур, Ван, 1962). *То же имеет место для общей игры «домино»* (Бергер, 1967).

В каждом случае к цели приводит одиа и та же идея доказательства. Мы сформулируем ее здесь для случая угловой игры «домиио». Каждой таблице Тьюринга T можно эффективным образом сопоставить угловую игру «домино» $\mathfrak{D}_T, \mathfrak{D}_T^0$ так, чтобы имела место эквивалентность

(5.1) $M(T)$ после применения к пустой ленте никогда не останавливается в том и только в том случае, когда $\mathfrak{D}_T, \mathfrak{D}_T^0$ — правильная игра.

Предположив теперь, что существует какой-то алгоритм, посредством которого можно было бы для произвольной угловой игры «домино» установить, правильная она или нет, мы бы смогли ввиду (5.1) и для произвольной таблицы Тьюринга T решить, останавливается ли $M(T)$ после применения к пустой ленте через конечное число шагов или нет. Но это свойство неразрешимо.

Эквивалентность (5.1) будет доказана нами в § 6, 7 и 8. $\mathfrak{D}_T, \mathfrak{D}_T^0$ обладают тем свойством, что существует не более одного когерентного углового покрытия посредством $\mathfrak{D}_T, \mathfrak{D}_T^0$. Если $M(T)$ после применения к пустой ленте никогда не останавливается и ввиду этого, согласно (5.1), существует когерентное угловое покрытие посредством $\mathfrak{D}_T, \mathfrak{D}_T^0$, то k-я строка этого покрытия тесно связана с k-й конфигурацией машины $M(T)$ (по поводу понятия конфигурации см. статью о машинах Тьюринга I, § 2).

Если вместо угловой игры «домино» мы рассмотрим диагональную игру «домино», то получим аналог (5.1). Доказательство этого факта труднее. В этом случае не удается добиться того, чтобы существовало не более одного когерентного диагонального покрытия посредством $\mathfrak{D}_T, \mathfrak{D}_T^0$ (например, мы получим другие когерентные диагональные покрытия, выбросив из когерентного диагонального покрытия первые s строк и s столбцов). Здесь имеется связь между k-ми диагоналями (нулевая диагональ есть главная диагональ) и k-й конфигурацией; см. об этом в § 13.

Труднее всего доказывается аналог (5.1) для общей игры «домино», так как здесь не существует геометрически выделенного поля, соответствующего начальной конфигурации.

§ 6. *Сопоставление таблице Тьюринга угловой игры «домино»* $\mathfrak{D}_T, \mathfrak{D}_T^0$

Пусть дана произвольная таблица Тьюринга T над алфавитом $0, \ldots, N$ с состояниями $0, \ldots, M$. Пусть 0 есть начальное состояние. $M(T)$ работает с бесконечной в одну сторону лентой, ячейки которой пронумерованы числами 0, 1, 2, ... Строка T имеет вид

$$qavq',$$

где q — исходное состояние, a — буква из рабочей ячейки, v — действие, определяемое q и a (a' или $\boldsymbol{r}$, или $\boldsymbol{l}$, или $\boldsymbol{s}$),

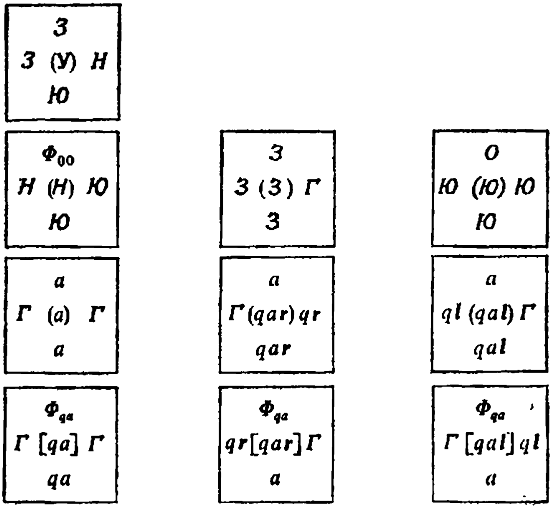


Рис. 2. Угловое домино (У) и другие домино из множеств $\mathfrak{D}_T$, $\mathfrak{D}_T^0$.

и q' — следующее состояние. Рассмотрим конфигурацию C; пусть в ячейке j находится буква a_j ($j = 0, 1, 2, \ldots$), ячейка n — текущая рабочая ячейка, q — текущее состояние:

$$C = q_0 \ldots a_{n-1} a_n^q a_{n+1} \ldots = a_0 \ldots a_n^q \ldots .$$

Таким образом, начальная конфигурация, когда машина $M(T)$ применяется к пустой ленте, имеет вид

$$C_0 = 0^0 000 \ldots . \tag{6.0}$$

В качестве *цветов* мы используем a, qa, $q\boldsymbol{r}$, $q\boldsymbol{l}$, $qa\boldsymbol{r}$, $qa\boldsymbol{l}$ (где a пробегает множество $\{0, \ldots, N\}$, а q — множество $\{0, \ldots, M\}$), а также З (запад), Н (начало), Г (горизонтальный), Θ (стоп). Мы введем зависящую от

T двуместную *функцию раскраски* Φ. Областью определения Φ является множество всех пар qa. Значением Φ_{qa} является цвет, который определяется исходя из таблицы T:

$$
(6.1)\qquad \Phi_{qa}=\begin{cases} q'a', & \text{если } qaa'q' \text{ есть строка } T,\\ q'ar, & \text{если } qarq' \text{ есть строка } T,\\ q'al, & \text{если } qalq' \text{ есть строка } T,\\ \Theta, & \text{если } qasq' \text{ есть строка } T.\end{cases}
$$

Типы домино, из которых состоят множества $\mathfrak{D}_T$, $\mathfrak{D}_T^0$, показаны на рис. 2. В центре квадрата указано имя соответствующего типа домино. Множество $\mathfrak{D}_T^0$ состоит только из одного «углового домино» (У). Если принять во внимание, что q пробегает числа $0, \ldots, M$ и a — числа $0, \ldots, N$, то очевидно, что $\mathfrak{D}_T$ содержит $5(N+1)(M+1)+(N+1)+4$ элементов.

Доказательство утверждения (5.1) будет дано в § 7 и 8.

§ 7. Лемма. Если $M(T)$ после применения к пустой ленте не останавливается, то угловая игра «домино» $\mathfrak{D}_T$, $\mathfrak{D}_T^0$ правильная

Доказательство. Мы будем строить когерентное (угловое) покрытие полосами. При этом мы опишем только несколько (горизонтальных) полос. Начальная полоса S_0 описывается следующим образом:

$$S_0=(\text{У})(\text{Н})(\text{Ю})(\text{Ю})(\text{Ю})\ \ldots\ .$$

Каждой конфигурации

$$C=a_0\ \ldots\ a_n^q\ \ldots$$

мы сопоставляем *три полосы* S_{Cd}, S_{Cr}, S_{Cl} (буква d должна ассоциироваться с «печатью»[1]):

$$
\begin{aligned}
S_{Cd}&=(\text{З})(a_0)\ldots(a_{n-1})[qa_n](a_{n+1})\ldots,\\
S_{Cr}&=(\text{З})(a_0)\ldots(qa_{n-1}r)[qa_nr](a_{n+1})\ldots,\\
S_{Cl}&=(\text{З})(a_0)\ldots(a_{n-1})[qa_nl](qa_{n+1}l)\ldots,
\end{aligned}
$$

[1]) «drucken» (нем.). — *Прим. перев.*

где на неописанных местах стоят домино (a) с соответствующими a. S_{Cr} определена только тогда, когда $n \geqslant 1$ (для того чтобы было возможно поместить домино ($qa_{r-1}\boldsymbol{r}$)).

Рассмотрим теперь S_0. Правый цвет (У) есть Н, и он совпадает с левым цветом (Н). Правый цвет (Н) совпадает с левым цветом (Ю), а именно с Ю. Наконец, правый цвет (Ю) совпадает с левым цветом (Ю). Итак, полоса S_0 по горизонтали когерентна. Непосредственной проверкой нетрудно убедиться в том, что все полосы S_{Cd}, S_{Cr} и S_{Cl} также когерентны по горизонтали. Наконец, можно установить, что при заданной конфигурации C последовательности *верхних* цветов полос S_{Cd}, S_{Cr} и S_{Cl} совпадают между собой, а именно:

$$(7.1) \qquad З a_0 \ldots a_{n-1} \Phi_{qa_n} a_{n+1} \ldots .$$

После этих приготовлений предположим, что $M(T)$ работает бесконечно долго. Тогда эта машина пробегает последовательность конфигураций C_0, C_1, C_2, ... Для каждого $j \geqslant 1$ пусть $v_j = \boldsymbol{d}$, соответственно $\boldsymbol{r}$, соответственно $\boldsymbol{l}$, в зависимости от того, какой вид имеет строка $qavq'$ таблицы T, которая ответственна за *переход от* C_{j-1} *к* C_j: $v = a'$ (для некоторого $a' \in \{0, \ldots, N\}$), либо $v = \boldsymbol{r}$, либо $v = \boldsymbol{l}$. Теперь мы покрываем квадрант полосами по следующей схеме:

$$\begin{array}{|l}
\ldots \\
S_{C_3 v_3} \\
S_{C_2 v_2} \\
S_{C_1 v_1} \\
S_0 \\
\hline
\end{array}$$

Наша цель будет достигнута, как только мы покажем, что это покрытие когерентно. Для этого необходимо проверить только когерентность по вертикали.

Пусть

$$(7.2) \qquad C_j = a_0 \ldots a_n^q \ldots .$$

Тогда последовательность верхних цветов $S_{C_j v_j}$ имеет вид (7.1). Заметим, что начальная конфигурация C_0 определена согласно (6.0); отсюда видно, что последовательность верхних цветов начальной полосы S_0 также имеет вид (7.1) (где $n=0$, $q=0$, $a_j=0$ для всех j). Итак, начальная полоса будет также включена в доказательство вертикальной когерентности, если удастся показать, что

(7.3) для каждого j ($j=0, 1, 2, \ldots$) имеет место утверждение: последовательность нижних цветов полосы $S_{C_{j+1}v_{j+1}}$ совпадает с (7.1).

Чтобы доказать это, нужно определить сначала C_{j+1}. Эта конфигурация зависит от строки qa_nvq' таблицы T. Мы рассмотрим здесь только случай $v=\boldsymbol{l}$. Случаи $v=\boldsymbol{r}$ и $v=a'$ проверяются совершенно аналогично; $v=\boldsymbol{s}$ невозможно, так как $M(T)$ после начала работы не останавливается.

Итак, допустим, что

$$qa_n\boldsymbol{l}q' \in T.$$

Отсюда следуют утверждения

(1) $\Phi_{qa_n}=q'a_n\boldsymbol{l}$.

(2) $v_{j+1}=\boldsymbol{l}$.

(3) $n \geqslant 1$ (иначе $M(T)$ остановится).

(4) $C_{j+1}=a_0\ldots a_{n-1}^{q'}\ldots$.

(5) $S_{C_{j+1}v_{j+1}}=(3)(a_0)\ldots[q'a_{n-1}\boldsymbol{l}]\,(q'a_n\boldsymbol{l})(a_{n+1})\ldots$.

(6) Нижние цвета этой полосы образуют последовательность $3a_0 \ldots a_{n-1},\ q'a_n\boldsymbol{l},\ a_{n+1}\ldots$.

Принимая во внимание (1), мы видим, что, согласно (6), нижние цвета $S_{C_{j+1}v_{j+1}}$ образуют последовательность (7.1).

§ 8. *Лемма. Если угловая игра «домино» $\mathfrak{D}_T$, $\mathfrak{D}_T^0$ правильная, то машина $M(T)$ после применения к пустой ленте никогда не останавливается*

Доказательство. Предположим, что $\mathfrak{D}_T$, $\mathfrak{D}_T^0$ правильная игра. Тогда существует когерентное угловое покрытие $\mathfrak{P}$. Для дальнейшего удобно занумеровать горизонтальные полосы, из которых составлено покрытие $\mathfrak{P}$, числами последовательности 0, 1, 2, ... Самая нижняя из полос является, таким образом, нулевой полосой. Вместе с тем домино внутри каждой полосы должны быть перенумерованы последовательностями чисел $-1, 0, 1, 2, \ldots$. Находящееся левее всех домино каждой полосы имеет, таким образом, номер -1. Пусть k-е домино j-й полосы $\mathfrak{P}$ есть d_{jk}. Таким образом, $d_{0,-1}$ есть угловое домино.

Мы покажем теперь индукцией по $j = 0, 1, 2, \ldots$, что

(1) $M(T)$ после применения к пустой ленте делает по крайней мере j шагов;

(2) если $C_j = a_0 \ldots a_n^q \ldots$ есть j-я конфигурация $M(T)$, то верхние цвета j-й полосы $\mathfrak{P}$ образуют последовательность $З a_0 \ldots \Phi_{qa_n} a_{n+1} \ldots d_{j,-1}$. Таким образом, верхний цвет $d_{j,-1}$ есть З, верхний цвет d_{jn} есть Φ_{qa_n}, и при $k \neq -1$, n верхний цвет d_{jk} есть a_k.

Тем самым из (1) непосредственно следует, что $M(T)$ работает бесконечно долго, что и доказывает лемму. (2) является лишь вспомогательным утверждением. Из доказательства (2) следует, что $\mathfrak{P}$ — единственное когерентное покрытие.

Для $j = 0$ утверждение (1) тривиально. (2) можно доказать следующим образом. Так как (У) — единственный элемент $\mathring{\mathfrak{D}}_T$, то имеем $d_{0,-1} = $ (У). Правый цвет (У) есть Н. Единственное домино, для которого Н есть левый цвет, — это (Н). Итак, $d_{00} = $ (Н). Подобным образом легко установить, что все следующие домино нулевой полосы совпадают с (Ю). Таким образом, нулевая полоса имеет вид (У)(Н)(Ю)(Ю)(Ю) ...; ее верхние цвета образуют последовательность $З\Phi_{00}000 \ldots$. Сравнив эту последовательность с нулевой конфигурацией $0^0000 \ldots$, видим, что (2) выполняется.

Переход от j *к* $j+1$. Индуктивное предположение состоит в том, что $M(T)$ совершает не менее j шагов и что верхние цвета j-й полосы $\mathfrak{P}$ образуют последовательность $З\, a_0 \ldots \Phi_{qa_n} a_{n+1} \ldots$, в то время как $C_j = a_0 \ldots a_n^q \ldots$ есть j-я конфигурация $M(T)$.

За $(j+1)$-й шаг ответственна строка таблицы T, начинающаяся символами qa_n. Пусть это есть строка $qa_n vq'$. Мы рассмотрим в пунктах от (a) до (d) все случаи для v и покажем, что (1) и (2) имеют место для каждого случая, согласующегося с существованием когерентного покрытия $\mathfrak{P}$.

(a) $v = s$. В этом случае $\Phi_{qa_n} = \Theta$ согласно (6.1). Таким образом, Θ есть верхний цвет d_{jn}. Тогда Θ должно было бы быть нижним цветом d_{j+1n}. Но домино с нижним цветом Θ вообще не существует. *Итак, случай* (a) *встретиться не может.*

(b) $v = a'$. При этом (1) выполняется тривиально. После $(j+1)$-го шага возникает конфигурация $C_{j+1} = a_0 \ldots a'^{q'} \ldots$, где a' находится в n-й ячейке. Таким образом, для доказательства (2) нужно показать, что верхние цвета $(i+1)$-й полосы образуют последовательность $3a_0 \ldots \Phi_{q'a'}a_{n+1} \ldots$.

По индуктивному предположению верхний цвет d_{jn} есть $\Phi_{qa_n} = q'a'$. Следовательно, нижний цвет d_{j+1n} должен быть $q'a'$. Этим $d_{j+1\,n}$ определено как $[q'a']$.

$d_{j+1\,n+1}$ имеет левый цвет Г, а нижний — a_{n+1}. Ввиду этого для $d_{j+1\,n+1}$ остаются лишь две возможности: домино (a_{n+1}) и домино вида $[q^*a_{n+1}l]$. Вторую возможность мы исключим: действительно, если бы $d_{j+1\,n+1} = [q^*a_{n+1}l]$, то левым цветом $d_{j+1\,n+2}$ был бы q^*l, а нижним — a_{n+2}. Но такого домино не существует. Тем самым показано, что $d_{j+1\,n+1} = (a_{n+1})$. Точно так же можно шаг за шагом показать, что $d_{j+1\,k} = (a_k)$ для всех $k > n+1$.

Теперь мы перейдем к определению домино d_{j+1k} при $k < n$. Для этого мы сначала предположим, что $n > 0$, и рассмотрим $d_{j+1\,n-1}$. У этого домино правый цвет совпадает с левым цветом $d_{j+1\,n}$, т. е. Г, а нижний цвет есть a_{n-1}. Этим условиям удовлетворяет домино (a_{n-1}) или домино вида $[q^*ar]$. Последнее невозможно, так как иначе правым цветом $d_{j+1\,n-2}$ был бы цвет q^*r и нижним — a_{n-2} (соответственно З, если $n = 1$), но таких домино не существует. Итак, $d_{j+1\,n-1} = (a_{n-1})$. У $d_{j+1\,n-1}$, как и у $d_{j+1\,n}$, левый цвет есть Г. Можно повторить рассуждения, которые привели нас к определению $d_{j+1\,n-1}$, и так шаг за шагом показать, что $d_{j+1\,k} = (a_k)$ для всех $k = n-1, \ldots, 0$. Наконец, у $d_{j+1,\,-1}$ правый цвет должен быть Г, а нижний — З. Этим условиям удовлетворяет только домино (З).

Таким образом, $(j+1)$-я полоса имеет вид (З)$(a_0) \ldots [q'a'](a_{n+1}) \ldots$; ее верхние цвета образуют последовательность $3a_0 \ldots \Phi_{q'a'}a_{n+1} \ldots$, что и требовалось доказать.

(c) $v=r$. (1) выполняется тривиальным образом. Возникает конфигурация $C_{j+1}=a_0 \ldots a_n a_{n+1}^{q'} a_{n+2} \ldots$. Таким образом, для доказательства (2) нужно показать, что верхние краски $(j+1)$-й полосы образуют последовательность $3a_0 \ldots a_n \Phi_{q'a_{n+1}} a_{n+2} \ldots$.

Верхняя краска d_{jn} есть $\Phi_{qa_n}=q'a_n r$. Из этого однозначно следует $d_{j+1\,n}=(q'a_n r)$.

Итак, $q'r$ есть левая, а a_{n+1} нижняя краска $d_{j+1\,n+1}$. Отсюда следует $d_{j+1\,n+1}=[q'a_{n+1}r]$. Левая краска $d_{j+1\,n+2}$ есть Г, а нижняя краска — a_{n+2}. Теперь, как и в (b), мы заключаем, что $d_{j+1\,k}=(a_k)$ для всех $k \geqslant n+2$. У $d_{j+1\,n-1}$ Г есть правая и a_{n-1}, соответственно 3,— нижняя краска. Пользуясь этим, можно, как и в (b), определить все $d_{j+1\,k}$ при $k<n$.

Итак, $(j+1)$-я полоса есть $(3)(a_0) \ldots [q'a_{n+1}r](a_{n+2}) \ldots$, ее верхние краски — $3a_0 \ldots a_n \Phi_{q'a_{n+1}} a_{n+2} \ldots$, что и требовалось доказать.

(d) $v=l$. Верхняя краска d_{jn} есть $\Phi_{qa_n}=q'a_n l$. Чтобы доказать (1), нужно исключить случай, когда $n=0$ (в противном случае $M(T)$ остановится ввиду «ухода за край ленты», ср. статью о машинах Тьюринга I, § 2). При $n=0$ нижняя краска $d_{j+1\,0}$ была бы $q'a_0 l$. Отсюда следует, что $d_{j+1\,0}=(q'a_0 l)$. Тогда правой краской $q_{j+1,-1}$ была бы $q'l$, а нижней — 3. Но такого домино не существует. Итак, $n>0$ и имеет место (1). Возникает новая конфигурация $C_{j+1}=a_0 \ldots a_{n-1}^{q'} a_n \ldots$.

Для доказательства (2) нужно показать, что верхние цвета $(j+1)$-й полосы образуют последовательность $3a_0 \ldots \Phi_{q'a_{n-1}} a_n \ldots$.

Как уже было отмечено, верхний цвет d_{jn} есть $q'a_n l$. Этим $d_{j+1\,n}$ определяется однозначно: $d_{j+1\,n}=(q'a_n l)$. Тогда левый цвет $d_{j+1\,n+1}$ есть Г и нижний цвет a_{n+1}. Теперь, как и в (b), заключаем, что $d_{j+1\,k}=(a_k)$ для всех $k \geqslant n+1$.

Мы знаем, что $n>1$. Правый цвет $d_{j+1\,n-1}$ есть $q'l$, а нижний цвет — a_{n-1}. Отсюда следует $d_{j+1\,n-1}=[q'a_{n-1}l]$. Тогда правый цвет $d_{j+1\,n-2}$ есть Г, а нижний цвет a_{n-2}, соответственно 3. Отсюда, как и в (b), можно определить все $d_{j+1\,k}$ для всех $k<n-1$.

Таким образом, $(j+1)$-я полоса есть $(3)(a_0) \ldots [q'a_{n-1}l]$ $(q'a_n l)\, a_{n+1} \ldots$; ее верхние цвета образуют последовательность $3a_0 \ldots \Phi_{q'a_{n-1}} a_n a_{n+1} \ldots$, что и требовалось доказать.

На рис. 3 изображены несколько первых домино когерентного покрытия посредством $\mathfrak{D}_T$, $\mathring{\mathfrak{D}}_T$ для машины $M(T)$, которая не останавливается, если применить ее к пустой ленте, и таблица которой содержит среди прочих строки $00r1$, 1012, $21l3$, 3014. Домино, соответствующие рабочим ячейкам,— это (Н), а также домино вида $[qa]$, соответственно $[qar]$, соответственно $[qal]$. Домино вида (qar), соответственно (qal), служат для «переноса информации». Заметим, что этот «перенос информации» возможен только через общие стороны домино.

(3)	[41]	(1)	(0)	(0)
(3)	[30l]	(31l)	(0)	(0)
(3)	(0)	[21]	(0)	(0)
(3)	(10r)	[10r]	(0)	(0)
(У)	(Н)	(Ю)	(Ю)	(Ю)

Рис. 3. Пример когерентного покрытия.

§ 9. *Определение выражения* $\alpha_{\mathfrak{D},\mathfrak{D}^0}$, *соответствующего угловой игре «домино»* $\mathfrak{D}$, $\mathfrak{D}^0$

Каждой угловой игре «домино» мы эффективным образом сопоставим выражение $\alpha_{\mathfrak{D},\mathfrak{D}^0}$, так чтобы имело место утверждение:

(9.1) Угловая игра «домино» $\mathfrak{D}$, $\mathfrak{D}^0$ правильна тогда и только тогда, когда $\alpha_{\mathfrak{D},\mathfrak{D}^0}$ выполнимо.

Эта эквивалентность будет доказана в § 10 и 11. Из нее следует неразрешимость свойства выполнимости выражения $\alpha_{\mathfrak{D}, \mathfrak{D}_0}$, так как иначе можно было бы решить, является ли правильной угловая игра «домино», что, как мы уже показали, невозможно.

Выражения $\alpha_{\mathfrak{D}, \mathfrak{D}_0}$ не принадлежат к узкой логике предикатов, так как они содержат функциональные переменные. В § 12 мы каждому выражению $\alpha_{\mathfrak{D}, \mathfrak{D}_0}$ эффективным образом сопоставим выражение $\varphi_{\mathfrak{D}, \mathfrak{D}_0}$ из класса выражений $\bigvee \wedge \bigwedge \bigvee \bigwedge$ (ср. в связи с этим § 4). Тем самым мы получаем принадлежащую Бюхи теорему:

Теорема. *Проблема разрешимости для класса выражений $\bigvee \wedge \bigwedge \bigvee \bigwedge$ не имеет решения. Этот класс является редукционным классом.*

В связи с классом выражений $\bigwedge \bigvee \bigwedge$ ср. § 13.

Пусть $\mathfrak{D} = \{d_1, \ldots, d_s\}$, $\mathfrak{D}_0 = \{d_1, \ldots, d_r\}$ $(r \leqslant s)$. Пусть стороны домино окрашены в цвета $c_1, \ldots, c_t$. Пусть верхний, правый, нижний и левый цвета d_n суть

$$c_{h_1(n)},\ c_{h_2(n)},\ c_{h_3(n)},\ c_{h_4(n)} \quad (n = 1, \ldots, s).$$

Выражение $\alpha_{\mathfrak{D}, \mathfrak{D}_0}$ есть конъюнкция определяемых далее выражений (9.1), ..., (9.7). Для построения этих выражений используют попарно различные символы двуместных предикатов $D_1, \ldots, D_s, C_1^1, \ldots, C_1^4, \ldots, C_t^1, \ldots, C_t^4$, символ одноместного предиката Z и одноместный функциональный символ f. (По поводу значения этих символов и определяемых далее выражений см. § 10.) Для более удобной записи этих выражений мы используем метаязыковый оператор единственности $(\bigvee ! p)$ «существует единственное p»). Если $\alpha_1, \ldots, \alpha_{p_0}$ — данные выражения, то $(\bigvee ! p)\, \alpha_p$ означает

$$(\alpha_1 \vee \ldots \vee \alpha_{p_0}) \wedge \neg(\alpha_1 \wedge \alpha_2) \wedge \ldots \wedge \neg(\alpha_1 \wedge \alpha_{p_0}) \wedge \ldots \\ \ldots \wedge \neg(\alpha_{p_0-1} \wedge \alpha_{p_0})).$$

Таким образом, $(\bigvee ! p)\, \alpha_p$ означает, что выполняется точно одно выражение α_p. Область, к которой принадлежит p_0, будет каждый раз ясна из контекста. Пусть x и y — фиксированные индивидные символы, Однозначность набора домино:

(9.1) $$\bigwedge x \bigwedge y (\bigvee ! n) D_n xy.$$

Однозначность набора цветов:

(9.2) $$\bigwedge x \bigwedge y (\bigvee ! m) C^1_m xy \wedge \ldots \wedge \bigwedge x \bigwedge y (\bigvee ! m) C^4_m xy.$$

Отношения для цветов домино:

(9.3_n) $$\bigwedge x \bigwedge y (D_n xy \rightarrow (C^1_{h_1(n)} xy \wedge \ldots \wedge C^4_{h_4(n)} xy))$$
($n = 1, \ldots, s$; всего s выражений!).

Горизонтальная когерентность:

(9.4_m) $\bigwedge x \bigwedge y (C^2_m xy \rightarrow C^4_m f xy)$ ($m = 1, \ldots, t$; всего t выражений!).

Вертикальная когерентность:

(9.5_m) $\bigwedge x \bigwedge y (C^1_m xy \rightarrow C^3_m x f y)$ ($m = 1, \ldots, t$; всего t выражеиий!).

Угловое условие:

(9.6) $$\bigwedge x \bigwedge y ((Zx \wedge Zy) \rightarrow (D_1 xy \vee \ldots \vee D_r xy)).$$

Существование нуля:

(9.7) $$\bigvee x Zx.$$

§ 10. *Лемма. Если угловая игра «домино» $\mathfrak{D}$, $\mathfrak{D}^0$ правильная, то $\alpha_{\mathfrak{D}, \mathfrak{D}^0}$ выполнимо*

При *доказательстве* будем исходить из фиксированного когерентного покрытия $\mathfrak{P}$ посредством $\mathfrak{D}$, $\mathfrak{D}^0$; используя это покрытие, мы построим интерпретацию $\mathfrak{J}$, в которой выполняется $\alpha_{\mathfrak{D}, \mathfrak{D}^0}$. В качестве совокупности индивидов B мы возьмем множество целых чисел $0, 1, 2, \ldots$. Поля первого квадранта мы занумеруем парами чисел, как показано на рис. 4.

(Отметим, что эта нумерация в двух отношениях отличается от принятой в § 8: нумерация всегда начииается с 0 и выбран обратный порядок компонент.) Мы определим интерпретацию I предикатов $D_1, \ldots, C^1_1, \ldots, Z$ и функции f следующим образом (при этом Rkl является сокращением утверждения, что числа k и l находятся в отношении R):

$I(D_n)kl$ тогда и только тогда, когда в $\mathfrak{P}$ на поле kl находится домино d_n.

$I(C^i_m)kl$ тогда и только тогда, когда i-я сторона домино, находящегося в $\mathfrak{P}$ на поле kl, окрашена в цвет c_m. При этом числа $r=1, 2, 3, 4$ обозначают верхнюю, правую, нижнюю, левую стороны соответственно.

$I(Z)k$ тогда и только тогда, когда $k=0$.

$I(f)(k)$ есть число $k+1$.

02	12	22
01	11	21
00	10	20

Рис. 4. Нумерация полей первого квадранта.

Теперь нетрудно проверить, что *выражения* (9.1), ..., (9.7) (*а следовательно, и* $\alpha_{\mathfrak{S}, \mathfrak{S}_0}$) *выполняются при* $\mathfrak{I} = \langle B, I \rangle$. А именно, выполняются выражения:

(9.1), так как на каждом поле находится единственное домино $\mathfrak{P}$;

(9.2), так как для каждого поля каждая сторона находящегося на нем домино окрашена в единственный цвет;

(9.3), так как для каждого поля и каждого $n=1, \ldots, s$ справедливо утверждение: если на поле находится домино d_n, то i-я сторона этого домино окрашена в цвет $c_{h_i(m)}$ (это справедливо для любого домино независимо от его местонахождения);

(9.4$_m$) для каждого m, так как для каждого поля справедливо утверждение: правый цвет находящегося на этом поле домино совпадает с левым цветом домино, расположенного справа от первого;

(9.5_m) для каждого m, так как для каждого поля имеет место утверждение: верхний цвет находящегося на этом поле домино совпадает с нижним цветом домино, расположенного выше первого;

(9.6), так как на поле 00 находится некоторое домино из набора $d_1, \ldots, d_r$;

(9.7), так как существует целое число, равное нулю.

§ 11. Лемма. Угловая игра «домино» $\mathfrak{D}$, $\mathfrak{D}^0$ правильна, если $\alpha_{\mathfrak{D},\,\mathfrak{D}^0}$ выполнимо

Для *доказательства* мы будем исходить из интерпретации $\mathfrak{J} = \langle B,\ I\rangle$, в которой выполняются все выражения (9.1), ..., (9.7). Множество B бесконечно или конечно, но в любом случае непусто (см. § 3). Интерпретация I сопоставляет символам D_n, C^i_m, Z некоторые отношения над B; обозначим их через $\underline{D}_n$, $\underline{C}^i_m$, $\underline{Z}$. Пусть $\underline{f}$ есть функция, которая сопоставляется символу f в силу I.

Так как (9.7) выполняется в силу $\mathfrak{J}$, то существует элемент B, для которого имеет место $\underline{Z}$. Возьмем такой элемент e и зафиксируем его. Итак, имеет место $\underline{Z}e$. Пусть $\underline{f}^0(e) = e$, $\underline{f}^{k+1}(e) = \underline{f}(\underline{f}_k(e))$ $(k = 0, 1, 2, \ldots)$. Каждый элемент $\underline{f}^k(e)$ принадлежит B.

Мы определим теперь покрытие $\mathfrak{P}$ первого квадранта набором домино $d_1, \ldots, d_s$. $\mathfrak{P}$ зависит от интерпретации $\mathfrak{J}$ и от выбора $e \in B$. Пусть kl есть произвольное поле. Покрытие $\mathfrak{P}$ определяется тем, какое домино должно находиться на этом поле. Так как (9.1) выполняется в интерпретации $\mathfrak{J}$, то существует единственное n, для которого $\underline{D}_n\underline{f}^k(e)\,\underline{f}^l(e)$. Пусть, скажем, $\underline{D}_{n_\bullet}\underline{f}^k(e)\,\underline{f}^l(e)$. Тогда на поле kl должно находиться домино $d_{n_\bullet}$. Осталось показать, что определенное таким образом покрытие $\mathfrak{P}$ когерентно и что на поле 00 находится домино из набора $d_1, \ldots, d_r$.

Так как (9.6) выполняется в интерпретации $\mathfrak{J}$, то в связи с $\underline{Z}e$ выполняется высказывание $\underline{D}_1ee$ или ... или $\underline{D}_ree$, т. е. $\underline{D}_1\underline{f}^0(e)\,\underline{f}^0$ или ... или $\underline{D}_r\underline{f}^0(e)\,\underline{f}^0(e)$. Итак, на поле 00 находится домино из набора $d_1, \ldots, d_r$, т. е. угловое условие выполнено.

Для доказательства горизонтальной когерентности $\mathfrak{P}$ мы используем тот факт, что (9.4) выполняется в интерпретации $\mathfrak{J}$ (вертикальная когерентность соответственно следует из (9.5)). Рассмотрим поля kl и $(k+1)l$. На поле kl в соответствии с $\mathfrak{P}$ находится домино d_{n_1}, иа поле $(k+1)l$ — домино d_{n_2}. Нужно показать, что эти домино соприкасаются между собой одинаковыми цветами, т. е. что правый цвет $c_{h_2(n_1)}$ домино d_{n_1} совпадает с левым цветом $c_{h_4(n_2)}$ домииo d_{n_2}.

Согласно определению $\mathfrak{P}$ выполняются оба отношения $\underline{D}_{n_1}\underline{f}^k(e)\underline{f}^l(e)$ и $\underline{D}_{n_2}\underline{f}^{k+1}(e)\underline{f}^l(e)$. В интерпретации $\mathfrak{J}$ выполняются (9.3$_{n_1}$) и (9.3$_{n_2}$). В частности, имеем $\underline{C}^2_{h_2(n_1)}\underline{f}^k(e)\underline{f}^l(e)$ и $\underline{C}^4_{h_4(n_2)}\underline{f}^{k+1}(e)\underline{f}^l(e)$. В интерпретации $\mathfrak{J}$ выполняется (9.4$_{h_2(n_1)}$). Поэтому из $\underline{C}^2_{h_2(n_1)}\underline{f}^k(e)\underline{f}^l(e)$ следует $\underline{C}^4_{h_2(n_1)}\underline{f}(\underline{f}^k(e))\underline{f}^l(e)$, т. е. $\underline{C}^4_{h_2(n_1)}\underline{f}^{k+1}(e)\underline{f}^l(e)$. Наконец, в интерпретации $\mathfrak{J}$ выполняется (9.2). Поэтому существует единственное m, для которого $\underline{C}^4_m\underline{f}^{k+1}(e)\underline{f}^l(e)$. Итак, мы получаем как $\underline{C}^4_{h_2(n_1)}\underline{f}^{k+1}(e)\underline{f}^l(e)$, так и $\underline{C}^4_{h_4(n_2)}\underline{f}^{k+1}(e)\underline{f}^l(e)$. Следовательно, $h_2(n_1)=h_4(n_2)$, что и требовалось доказать.

§ 12. *Переход к узкой логике предикатов*

Выражение $\alpha_{\mathfrak{T},\mathfrak{T}^*}$, т. е. конъюнкция выражений (9.1), … …, (9.7), замкнуто (ср. § 2). Символ f встречается только в формулах (9.4$_m$) и (9.5$_m$). В выражениях (9.4$_m$) мы имеем fx, в выражениях (9.5$_m$) — fy. Заметим теперь, что (9.5$_m$) эквивалентно

$$(9.5'_m) \qquad \bigwedge x \bigwedge y\,(C^1_m yx \longrightarrow C^3_m y f x),$$

так что после замены выражения (9.5$_m$) на (9.5$'_m$) символ f встречается только в сочетании fx.

Заметим, что, согласно элементарному правилу логики, выражение $(\bigwedge x \bigwedge y\,\beta_1 \wedge \bigwedge x \bigwedge y\,\beta_2)$ эквивалентно выражению $\bigwedge x \bigwedge y\,(\beta_1 \wedge \beta_2)$; ввиду этого мы эффективным образом получаем из (9.1), …, (9.5$'_m$), …, (9.7) эквивалентное

$\alpha_{\mathfrak{T},\,\mathfrak{T}^0}$ замкнутое выражение вида

$$\bigvee x\, Zx \wedge \bigwedge x \bigwedge y \beta, \tag{9.8}$$

где β свободно от кванторов и содержит f только в сочетании fx. Нам осталось исключить символ f.

Для этой цели мы следующим образом используем процедуру Сколема. Пусть z есть индивидный символ, отличный от x и y. Выражение γ получается из β после замены всюду в β терма fx символом z. Образуем выражение

$$\bigvee x\, Zx \wedge \bigwedge x \bigvee z \bigwedge y \gamma; \tag{9.9}$$

мы утверждаем, что (9.9) и (9.8) равновыполнимы. Если это действительно так, то мы достигли желаемого (ср. § 9): выражение (9.9) можно рассматривать как выражение $\varphi_{\mathfrak{D},\,\mathfrak{D}^0}$ из класса выражений $\bigvee \wedge \bigwedge \bigvee \bigwedge$. Тем самым мы для каждой угловой игры «домино» $\mathfrak{D}$, $\mathfrak{D}^0$ эффективно построили выражение из этого класса, причем так, что это выражение выполнимо тогда и только тогда, когда игра $\mathfrak{D}$, $\mathfrak{D}^0$ правильна.

Для того чтобы подготовить доказательство равновыполнимости выражений (9.8) и (9.9), отметим несколько элементарных фактов о справедливости выражения в некоторой интерпретации. Положения (*) и (**) являются составными частями индуктивного определения справедливости (ср. § 3), в то время как (***) представляет собой один специальный случай «теоремы перенесения», связанной с подстановкой.

Пусть $\mathfrak{I} = \langle B, I\rangle$ есть произвольная интерпретация и a есть элемент B. Мы введем интерпретацию $\mathfrak{I}^a_x = \langle B, I^*\rangle$, где I^* определено для тех же символов, что и I, а также для (возможно, дополнительного) индивидного символа x. Для отличного от x символа, для которого I^* определена, I^* имеет то же значение, что и I. Пусть, наконец, $I^*(x) = a$. Предположим, что в (*) и (**) α есть выражение, x есть индивидный символ и $\mathfrak{I} = \langle B, I\rangle$ есть интерпретация выражения $\bigwedge x\alpha$ (или, что одно и то же, $\bigvee x\alpha$). Мы получим теперь

(*) $\bigwedge x\alpha$ имеет место в интерпретации $\mathfrak{I}$ тогда и только тогда, когда для всех a из B выражение α имеет место в интерпретации $\mathfrak{I}^a_x$;

(**) $\bigvee x\alpha$ имеет место в интерпретации $\mathfrak{J}$ тогда и только тогда, когда для некоторого a из B выражение α имеет место в интерпретации $\mathfrak{J}_x^a$.

Переходя к формулировке (***), мы предположим, что σ есть выражение, в которое входит индивидный символ z, причем каждое его вхождение является *свободным* (ср. § 2). Символ x должен входить в σ несвязанным образом. Выражение τ должно получаться из σ заменой каждого вхождения z на fx. (Заметим, что эти предположения выполняются для $\sigma = \bigwedge y\gamma$ и $\tau = \bigwedge y\beta$; ср. (9.8), (9.9).) Пусть $\mathfrak{J} = \langle B, I\rangle$ есть произвольная интерпретация τ. Пусть $b = I(f)(I(x))$ (отметим, что $I(f)$ и $I(x)$ определены). Тогда имеем

(***) τ имеет место в интерпретации $\mathfrak{J}$ тогда и только тогда, когда σ имеет место в интерпретации $\mathfrak{J}_z^b$.

После этих приготовлений будет показано, что (9.8) *и* (9.9) *равновыполнимы.*

(a) *Если выполнимо* (9.8), *то* (9.9) *также выполнимо.* (9.8) имеет место в интерпретации $\mathfrak{J} = \langle B, I\rangle$. Мы покажем, что в той же интерпретации имеет место и (9.9). Для этого достаточно показать, что в интерпретации $\mathfrak{J}$ имеет место $\bigwedge x \bigvee z \bigwedge y\gamma$. Имеем последовательно:

$\bigwedge x \bigwedge y\beta$ имеет место в интерпретации $\mathfrak{J}$, так как в $\mathfrak{J}$ имеет место (9.8);
для всех $a \in B$ $\bigwedge y\beta$ имеет место в $\mathfrak{J}_x^a$ ввиду (*);
для всех $a \in B$ $\bigwedge y\gamma$ имеет место в $\mathfrak{J}_{xz}^{ab}$ для некоторого $b \in B$ ввиду (***);
для всех $a \in B$ $\bigvee z \bigwedge y\gamma$ имеет место в $\mathfrak{J}_x^a$ ввиду (**);
$\bigwedge x \bigvee z \bigwedge y\gamma$ имеет место в $\mathfrak{J}$ ввиду (*).

(b) *Если* (9.9) *выполнимо, то выполнимо и* (9.8). (9.9) имеет место в $\mathfrak{J} = \langle B; I\rangle$. В выражении (9.9) в отличие от (9.8) функциональиый символ f не встречается. Поэтому никакого значения не имеет, *определено или нет значение* $I(f)$, а если оно определено, то *чему* равно $I(f)$. Этот факт мы используем для такого определения $I(f)$ (при случае изменив исходное определеиие), чтобы можно было показать, что (9.8) также выполняется в интерпретации $\mathfrak{J}$. Так как f не имеет вхождений в $\bigvee x Zx$, то достаточно показать, что $\bigwedge x \bigwedge y\beta$ имеет место в указанным образом измененной интерпретации $\mathfrak{J}$.

Мы исходим из того, что $\bigwedge x \bigvee z \bigwedge y\gamma$ имеет место в интерпретации $\mathfrak{J}$. Используя (*) и (**), получаем, что для каждого a из B существует по крайней мере одно b из B, такое, что $\bigwedge y\gamma$ имеет место в $\mathfrak{J}^{ab}_{xy}$. Согласно аксиоме выбора, существует определенная на B функция $\underline{f}$, такая, что для каждого a из B значение $\underline{f}(a)$ совпадает с определенным таким образом b. (Не обязательно пользоваться аксиомой выбора, так как можно показать (без этой аксиомы), что существует реализующая (9.9) интерпретация $\mathfrak{J} = \langle B, I\rangle$, в которой B перечислимо.) Положим $I(f) = \underline{f}$. Тогда $b = I(f)(a)$. Применив теперь (***) к $\sigma = \bigwedge y\gamma$, $\tau = \bigwedge y\beta$ и $\mathfrak{J} = \mathfrak{J}^a_x$, обнаружим, что из того, что $\bigwedge y\gamma$ имеет место в $\mathfrak{J}^{ab}_{xy}$, следует: $\bigwedge y\beta$ имеет место в $\mathfrak{J}^a_x$. Это справедливо для всех a. Итак, ввиду (*) выражение $\bigwedge x \bigwedge y\beta$ имеет место в $\mathfrak{J}$, что и требовалось доказать.

§ 13. Обзор проблемы разрешимости для класса выражений $\bigwedge \bigvee \bigwedge$ и диагональной игры «домино»

В § 9 мы сопоставили каждой *угловой игре «домино»* $\mathfrak{D}$, $\mathfrak{D}^0$ выражение $\alpha_{\mathfrak{D}, \mathfrak{D}^0}$ таким образом, что выполняется соотношение (9.1), как это уже было показано в § 10 и 11. Нетрудно подобным образом каждой *диагональной игре «домино»* $\mathfrak{D}$, $\mathfrak{D}^0$ сопоставить выражение $\bar{\alpha}_{\mathfrak{D}, \mathfrak{D}^0}$, такое, что

(13.1) Диагональная игра «домино» $\mathfrak{D}$, $\mathfrak{D}^0$ правильна тогда и только тогда, когда $\bar{\alpha}_{\mathfrak{D}, \mathfrak{D}^0}$ выполнимо.

Для построения выражения $\bar{\alpha}_{\mathfrak{D}, \mathfrak{D}^0}$ мы, как и в § 9, используем предикатные символы $D_1, \ldots, C_1^1, \ldots, C_1^4, \ldots$ и функциональный символ f, но не будем пользоваться предикатным символом Z. Выражение $\bar{\alpha}_{\mathfrak{D}, \mathfrak{D}^0}$ есть конъюнкция всех выражений (9.1), ..., (9.5_t) и некоторого дополнительного выражения, описывающего *условие диагональности*:

(13.2) $$\bigwedge x(D_1xx \vee \ldots \vee D_rxx).$$

(Угловое условие (9.6) и условие (9.7) отсутствуют.) Доказательство (13.1) может быть получено из доказательства (9.1) с немногими изменениями.

(a) Предположим, что диагональная игра «домино» $\mathfrak{D}$, $\mathfrak{D}^0$ правильна. Исходя из когерентного диагонального покрытия $\mathfrak{P}$ посредством $\mathfrak{D}$, $\mathfrak{D}^0$, образуем интерпретацию $\mathfrak{I}$, как и в § 10. Как и раньше, получаем теперь, что все выражения (9.1), ..., (9.5_t) имеют место в интерпретации $\mathfrak{I}$. Введенное ранее *диагональное условие* выполняется в интерпретации $\mathfrak{I}$, так как на каждом диагональном поле kk находится одно домино из набора $d_1, \ldots, d_r$. Итак, $\overline{\alpha}_{\mathfrak{D}, \mathfrak{D}^0}$ выполнимо.

(b) Пусть $\overline{\alpha}_{\mathfrak{D}, \mathfrak{D}^0}$ выполнимо. Мы будем исходить из интерпретации $\mathfrak{I} = \langle B, I \rangle$, в которой имеют место все выражения (9.1), ..., (9.5_t) и диагональное условие (13.2). *Пусть e обозначает произвольный элемент B.* Покрытие $\mathfrak{P}$ будет теперь определено в зависимости от $\mathfrak{I}$ и e, как в § 11. Когерентность $\mathfrak{P}$ следует из тех же соображений. Осталось показать, что на диагонали покрытия $\mathfrak{P}$ находятся только домино из множества $\mathfrak{D}^0$. Согласно предположению, диагональное условие (13.2) имеет место в интерпретации $\mathfrak{I}$. Ввиду этого для каждого элемента $p \in B$ имеем $\underline{D}_1 pp$ или ... или $\underline{D}_r pp$, так что, в частности, $\underline{D}_1 \underline{f}^k(e) \underline{f}^k(e)$ или ... или $\underline{D}_r \underline{f}^k(e) \underline{f}^k(e)$. Это означает, что на каждом диагональном поле kk находится одно из диагональных домино d_1 или ... или d_r.

Так как в диагональном случае элемент e может быть выбран из B произвольным образом, то доказательство (13.1) еще проще, чем его аналог для углового случая. Однако совсем по-другому обстоит дело с доказательством теоремы о неразрешимости диагональной проблемы. Мы не будем излагать здесь это доказательство, но сделаем несколько замечаний в связи с методом доказательства.

Пусть задана таблица Тьюринга T. Ей должна быть эффективиым образом сопоставлена диагональная игра «домино» $\mathfrak{D}_T$, $\mathfrak{D}_T^0$, правильная в том и только в том случае, когда $M(T)$ после применения к пустой ленте никогда не останавливается. Как и в случае угловой игры, игра «домино» должна быть устроена таким образом, чтобы было возможно из последовательности конфигураций бесконечно долго работающей машины $M(T)$ составить когерентное покрытие посредством $\mathfrak{D}_T$, $\mathfrak{D}_T^0$ и чтобы, обратно, по заранее заданному когерентному покрытию посредством $\mathfrak{D}_T$, $\mathfrak{D}_T^0$ можно было бы восстановить некоторую последовательность конфигураций, которая допускала бы интерпретацию как последовательность конфигураций, пробегаемая машиной $M(T)$ после применения ее к пустой ленте.

Уже в § 5 упоминалось, что j-я конфигурация должна быть «представлена» j-й диагональю ($j=0, 1, 2, \ldots$); j-я диагональ состоит из всех полей вида $k\,k+j$ (ср. рис. 4). Нулевая диагональ является главной диагональю. Покрытие полей, лежащих ниже главной диагонали, можно реализовать тривиальным образом, взяв в качестве элементов $\mathfrak{D}_T^0$ такие домино, чтобы их нижняя и правая стороны были окрашены в один цвет Н(«нижний») и чтобы в набор $\mathfrak{D}_T$ входило домино (Н), все стороны которого были бы окрашены в цвет Н (мы предполагаем, что цвет Н не встречается ни в каких других домино).

Если мы захотим попытаться представить, например, нулевую конфигурацию главной диагональю, подобно тому как в случае угловой игры мы представили нулевую конфигурацию нулевой полосой, то будет невозможно исключить существование тривиального когерентного покрытия посредством $\mathfrak{D}_T$, $\mathfrak{D}_T^0$ (ср. относящееся к этому вопросу замечание в конце § 5). Однако Кар, Мур и Ван заметили, что совсем необязательно представлять *всю* j-ю конфигурацию и что можно ограничиться конечным отрезком записи на ленте. Очевидно, достаточно рассмотреть поля $0, \ldots, j$. Одно из этих полей должно быть рабочим полем, а поля, лежащие правее j-го поля, еще «не обрабатывались машиной» и по-прежнему содержат символ 0. Соответствующий начальный отрезок нулевой конфигурации будет представлен периодической последовательностью домино на главной диагонали. На следующей диагонали будет периодически представлен вдвое больший начальный отрезок первой конфигурации и т. д. Цвета домино будут определяться не одной только машиной T, как это было в случае угловой игры. В частности, они будут содержать компоненту, которая и приводит ко все возрастающим периодам.

Мы удовлетворимся здесь этими указаииями о характере диагональной проблемы.

В § 12 мы построили замкнутое выражение узкой логики предикатов, равновыполнимое с $\alpha_{\mathfrak{D},\mathfrak{D}^0}$ и имевшее вид $\bigvee xZx \wedge \bigwedge x \bigvee z \bigwedge y\gamma$. Этим было показано, что проблема разрешимости для класса выражений $\bigvee \wedge \bigwedge \bigvee \bigwedge$ ие имеет решения (ср. § 9). Мы можем примеиить теперь к $\bar{\alpha}_{\mathfrak{D},\mathfrak{D}^0}$ ту же процедуру, посредством которой мы преобразовали в § 12 выражение $\alpha_{\mathfrak{D},\mathfrak{D}^0}$. Мы придем при этом к более простому выражению, так как в $\alpha_{\mathfrak{D},\mathfrak{D}^0}$ *не входит составная часть* $\bigvee xZx$ *конъюнкции*. Все остальные члены конъюнкции в $\bar{\alpha}_{\mathfrak{D},\mathfrak{D}^0}$, исключая (13.2), имеют вид $\bigwedge x \bigwedge y\delta$, причем символ f, если и входит в какой-нибудь из этих членов, то либо в связи с x, либо в связи с y. Выражение (13.2) допускает тривиальную замену эквивалентным выражением того же вида, если в (13.2) устранить лишние кванторы $\bigwedge y$ (ср. в связи с этим замечание в конце § 3).

Итак, мы можем эффективиым образом сопоставить выражению $\alpha_{\mathfrak{D},\mathfrak{D}^0}$ равновыполнимое замкнутое выражение узкой логики предикатов вида $\bigwedge x \bigvee z \bigwedge y\gamma$. В сочетанин с (13.1) это озиачает, что $\bigwedge \bigvee \bigwedge$ есть редукционный класс. Упрощенное доказательство Кара, Мура и Вана имеется, кроме того, в [7].

ЛИТЕРАТУРА

1. Wang H., Proving Theorems by Pattern Recognition II, *Bell Systems Tech. J.*, 40 (1961), 1—41.
2. Büchi J. R., Turing Machines and the Entscheidungsproblem, *Notices Amer. Math. Soc.*, 8 (1961), 354.
3. Büchi J. R., Turing Machines and the Entscheidungsproblem, *Math. Ann.*, 148 (1962), 201—213.
4. Kahr A. S., Moore E. F., Wang H., Entscheidungsproblem Reduced to the ∀∃∀ Case, *Proc. Nat. Acad. Sci USA*, 48 (1962), 365—377.
5. Berger R., The Undecidability of the Domino Problem, Memoirs Amer. Math. Soc. 66, 1966.
6. Hermes H., Einfürung in die mathematische Logik, 1969.
7. Hermes H., A Simplified Proof for the Unsolvability of the ∀∃∀-Case (в печати).
8. Ackermann, Solvable Cases of the Decision Problem, Amsterdam, 1957.
9. Surányi, Reduktionstheorie des Entscheidungsproblems im Prädikatenkalkül der ersten Stufe, Budapest, 1959.
10*. Чёрч А., Введеиие в математическую логику, ИЛ, М., 1960.
11*. Линдон Р. К., Заметки по логике, «Мир», М., 1968.

МАШИНЫ ТЬЮРИНГА И СЛУЧАЙНЫЕ 0-1-ПОСЛЕДОВАТЕЛЬНОСТИ

К. ЯКОБС

Предложите не слишком раздраженному человеку написать последовательность из тридцати нулей и единиц, или, как мы будем говорить, 0-1-слово $w = w_1 \ldots w_{30}$ длины $|w| = 30$; хотя он, по-видимому, и не напишет ряд

(1) $$000000000000000000000000000000,$$

но все же скорей всего это будет последовательность, в которой легко угадать некоторое правило ее построения, например такая:

$$010101010101010101010101010101$$

или с повторением через три:

$$001001001001001001001001001001;$$

возможно также, — хотя это уже более изощренный пример, — что и такая:

(2) $$010010001000010000010000001000.$$

Если его изобретательность пробуждена таким образом впервые, то он может найти удовольствие в придумывании все более сложных правил, и тогда довольно скоро окажется, что для того, чтобы проиллюстрировать эти правила, ему потребуются слова все большей и большей длины. Следующая последовательность, подробно рассмотренная в статье «Машинно-порожденные 0-1-последовательности» этой книги:

$$001001110001001110110110001001$$

подчиняется правилу, названному там «вальсом бесконечного порядка», которое, как и любое из приведенных выше правил, позволяет строить слова произвольной длины и тем самым — бесконечные 0-1-последовательности (естественно, что при длине слова $27=3^3$ это правило проявляется более наглядно, чем при длине 30).

Возможно, однако, что кто-нибудь спросит: зачем, собственно, нужно выбирать правило? Сделаем случайный выбор. Подбросив 30 раз монету и обозначив выпадение герба нулем, а решетки — единицей, мы получим, например, такую последовательность:

(3) 110101000011100100100101111111.

Эту последовательность тоже нельзя назвать совершенно беспорядочной. В ней легко заметить, например, определенную троекратную повторяемость символов или групп символов. Можно дать, например, такое описание этой последовательности:

Сначала 1, затем трижды 10, затем трижды 0, затем трижды 1, затем трижды 001, затем 0, затем семь раз 1.

Тем не менее это описание вряд ли проще изображения самого слова.

Как же выразить в точной форме такие понятия, как «слово с правильной структурой», «просто конструируемое слово», «случайное слово».

Колмогорову [8] принадлежит идея измерять сложность 0-1-слова наименьшей длиной его описаний.

Например, слово (1) допускает короткое описание: «одни нули» (независимо от того, что длина слова равна 30), и поэтому обладает малой сложностью. Для задания слова (2) потребуется уже больше слов, но описание «перед k-й единицей k нулей» является все еще достаточно кратким и определяет бесконечную 0-1-последовательность, из которой нужное 0-1-слово вырезается указанием длины. Слово (3) нуждается, как мы будем говорить, в длинном описании и поэтому обладает большой сложностью.

Естественно, что мы должны сначала уточнить эти все еще интуитивные рассуждения. Необходимо, во-первых, точно определить, что следует называть «описанием». Здесь в нашем распоряжении имеется развиваемая начиная с тридцатых годов теория вычислимости, т. е. теория машин

Тьюринга (или, что одно и то же, теория вычислимых по Тьюрингу функций) либо теория алгоритмов. Мы будем использовать эту теорию в объеме статьи «Машины Тьюринга и вычислимые функции I—III» этой книги и, таким образом, заранее предполагаем, что читатель знаком с этой статьей или с каким-нибудь другим аналогичным изложеиием (например, Мартин-Лёф [9], Хермес [6]). Однако нижеследующее можно воспринимать и на интуитивном уровне, и я хотел бы попытаться ориентировать стиль этой статьи иа такое интуитивное понимание. В основном достаточно представлять себе следующее:

1) «Описать» конечное 0-1-слово $w\,(=w_1\ \dots\ w_n)$ ($w_1, \dots, w_n = 0$ или 1) означает написать такую программу для какой-то машины, чтобы после ввода этой программы в машину она печатала слово w.

2) Мы будем обычно работать с программами, состоящими из двух частей, а именно: а) указания длины слова $n\,(=0,\ 1,\ 2,\ \dots)$ и b) остальпого описания.

Оба указания должны быть заданы в форме конечных 0-1-слов. Этого можно достичь, если длины слов n писать для машины в двоичном представлеиии (т. е. 0 вместо 0, 1 вместо 1, 10 вместо 2, 11 вместо 3 и т. д.), хотя мы будем здесь по-прежнему спокойно обозначать их числами $n = 0,\ 1,\ 2,\ \dots$, а остальное описание также закодировать 0-1-словом p.

Теперь программа представляет собой пару $(n,\ p)$ конечных 0-1-слов, причем n содержит по крайней мере один символ.

3) Мы работаем с машинами, являющимися машинами Тьюринга (см. части I—III первой статьи этой книги) и притом такими, которые после задаиия некоторой программы, если только они применимы к ней, печатают 0-1-слово $w = w_1\ \dots\ w_n$ длины $|w| = n$ (при $n = 0$ всегда пустое слово $w = \square$). Мы допускаем, что машина порождает не все слова, например примитивная машина, печатающая только n нулей независимо от вида p; мы также допускаем, что некоторые программы машина вообще не воспринимает.

4) В принципе важна не машина сама по себе, а соответствие $A\,(*|*) : (n,\ p) \longrightarrow A\,(p\,|\,n)$, которое она порождает; через $A\,(p\,|\,n)$ обозначается 0-1-слово длины n, печатаемое

после ввода программы (n, p). Таким образом, $A(*|*)$ есть некоторая *вычислимая по Тьюрингу функция*, определенная на некотором *подмножестве* $\Omega^2 = \Omega^2(\{0, 1\})$ всех упорядоченных пар конечных 0-1-слов (а именно, на множестве программ, воспринимаемых машиной) со значениями в множестве $\Omega = \Omega(\{0, 1\})$ всех конечных 0-1-слов, причем множество значений не совпадает со всем Ω: его элементы должны удовлетворять дополнительному условию

$$|A(p|n)| = n \qquad (n = 0, 1, \ldots)$$

(см. статью «Машины Тьюринга и вычислимые функции I—III» в этой книге). Тем не менее мы будем по-прежнему коротко говорить о «машине A» даже и в тех случаях, когда по существу нас будет интересовать вычислимая по Тьюрингу функция вышеописанного типа.

Тем самым мы приблизительно обрисовали ту форму, которую придал Колмогоров [8] своей идее, и одновременно бросили взгляд на теорию, которую мы хотим изложить в этой статье.

Источник возникновения этой теории — проблема обоснования теории вероятностей и продолжающееся, начиная с 1933 г., развитие связанных с этой проблемой идей фон Мизеса и Колмогорова. Стало уже обычным при теоретико-вероятностных рассмотрениях иметь дело со сложными математическими моделями для описания реальных явлений, которые мы считаем «случайными». Но типичные проблемы обоснования возникают уже в классическом эксперименте Бернулли — произвольно долго повторяющемся бросании идеальной монеты (Бернулли [1]); и если мы хотим построить математическую модель этого явления, то мы должны сопоставить гербу, скажем, символ 0, решетке — символ 1, а затем изучать либо конечные 0-1-последовательности произвольной длины, т. е. 0-1-*слова* $w = w_1 \ldots w_n$, либо *бесконечные* 0-1-*последовательности* $x = x_1x_2 \ldots$. Источник проблемы обоснования заключается в том, что для определения понятия «случайного слова» или «случайной последовательности» приходится привлекать некоторый физический процесс (бросание монеты), который не имеет никакого отношения к математике и с помощью которого не может быть определено никакое математическое свойство; наоборот, он сам нуждается в описании посредством какой-то математической модели. Таким образом, возникает задача — дать такое математическое определение понятиям «случайное 0-1-слово», «случайная 0-1-последовательность», чтобы теория, в основу которой положено это определение, давала те же результаты при описании экспериментов с бросанием монеты, что и существующая «нестрогая» теория. С самого начала было ясно, что прежде всего следует заняться определением понятия «беспорядочная последовательность», так как «беспорядочность» является основным признаком «случайности».

В связи с этим фон Мизес [11] предложил в 1919 г. называть бесконечную 0-1-последовательность $x = x_1 x_2 \ldots$ *случайной* последовательностью, или *коллективом*, если

I) относительная частота появления 1, т. е. $\lim\limits_{n\to\infty} \frac{1}{n}(x_1 + \ldots + x_n)$, равна $1/2$,

II) и (что является попыткой определения понятия «беспорядочный») это свойство сохраняется при переходе с использованием любого правила выбора к подпоследовательности:

$$\frac{1}{n}(x_{i_1} + \ldots + x_{i_n}) \longrightarrow \frac{1}{2} \quad (n \longrightarrow \infty).$$

Фон Мизес определял вероятности как пределы относительных частот и намеревался исследовать теорию вероятностей и в других ее аспектах как теорию преобразований данных коллективов. В 1936 г. фон Мизес вновь изложил свои идеи в книге [12][1]). Главная трудность для него состояла в точном выражении понятия «правило выбора». Вальду [16], [17] удалось получить такое уточнение и доказать, что для произвольной данной счетной совокупности правил выбора найдется континуум коллективов в смысле условий I, II, если в II ограничиться правилами выбора только из этой счетной совокупности. Однако в 1939 г. эта дискусия была прервана Виллем [15], указавшим конструкцию, позволяющую для

[1]) Чёрч [20] формализовал концепцию фон Мизеса на языке вычислимых функций. — *Прим. перев.*

каждой счетной совокупности правил выбора строить некоторую 0-1-последовательность $x = x_1 x_2 \ldots$, удовлетворяющую условиям I и II, но такую, что $\frac{1}{n}(x_1 + \ldots + x_n) \geqslant \frac{1}{2}$ ($n = 1, 2, \ldots$). Такие последовательности «предрасположены к 1», что не может иметь места для случайной последовательности; уже в 1924 г. в относящемся сюда разделе теории вероятностей была доказана теорема о двойном логарифме, утверждающая, что

$$\limsup_{n\to\infty} \frac{x_1 + \ldots + x_n - \frac{n}{2}}{\frac{1}{2}\sqrt{2n \log\log n}} = 1,$$

$$\liminf_{n\to\infty} \frac{x_1 + \ldots + x_n - \frac{n}{2}}{\frac{1}{2}\sqrt{2n \log\log n}} = -1.$$

В примерах Вилля второе из этих соотношений не выполняется. Очевидно, что развитие идеи фон Мизеса испытывало трудности потому, что к «коллективам» предъявлялось требование удовлетворять лишь *некоторым* из известных в обычной теории вероятностей предложений, и они не удовлетворяли другим. Отсутствовала идея, позволяющая связать между собой *все* предложения, как известные, так и те, которые еще предстояло открыть. В самом деле, всякое разумное определение понятия «случайная последовательность» должно было выдерживать в будущем любую возможную проверку.

Между тем предложение Колмогорова, сделанное им в 1933 г. [7], рассматривать теорию вероятностей как прикладную теорию меры (здесь имеется в виду, что мы больше не говорим об индивидуальных последовательностях, а только о множествах последовательностей) привлекло своей элегантностью и убедительностью большинство ученых, работавших в теории вероятностей. Развитие исследований, начатых фон Мизесом, остановилось, и в течение многих лет все усилия были направлены на усовершенствование и углубление теоретико-вероятностных концепций, ориентированных на теорию меры; итоги этого развития представлены в книгах Блюменталя—Гетоора

[2], Браймана [4], Дынкина [5]. Однако в 1965 г. теперь уже сам Колмогоров [8][1]) вновь рассмотрел первоначальную проблему и предложил в качестве меры «случайности» упоминавшуюся выше сложность конечных 0-1-слов w. Мы развиваем эти соображения в § 1, но, как мы покажем в § 2, непосредственное применение этой идеи не приводит ни к какому разумному определению понятия «случайная 0-1-последовательность»; теорема 2.2 (Мартин-Лёф [9]) показывает, что среди отрезков $x_1 \ldots x_n$ $(n=1, 2, \ldots)$ любой бесконечной 0-1-последовательности $x=x_1x_2 \ldots$ бесконечно много относительно упорядоченных.

Затем Мартин-Лёф [9], [10] определил случайные 0-1-последовательности как такие последовательности, которые удовлетворяют одному из так называемых универсальных *секвенциальных тестов*. Этим тестам удовлетворяет несчетное множество бесконечных 0-1-последовательностей, для которых выполняются все утверждения классической теории вероятностей, как уже известные, так и те, которые еще будут открыты. Каждое из этих утверждений добавляет к тесту свой «фильтр», сквозь который «просеиваются» только те последовательности, которые удовлетворяют этому утверждению (ср. также Шнорр [13], [14]).

Отмеченная здесь *универсальность* является существенным отличительным аспектом теории Колмогорова и Мартин-Лёфа. Ее нужно понимать в смысле теории Тьюринга. Там она находит свое выражение в теоремах о перечислимости по Тьюрингу множества всех перечислимых по Тьюрингу множеств (например, натуральных чисел): это есть так называемая теорема о перечислимости (см. часть III первой статьи этой книги (теорема 6.4) и статью о перечислимости (теорема 3.9)), которой мы будем постоянно пользоваться.

Стоит еще упомянуть, что требование *«симметричности»* монет, т. е. вероятности $^1/_2$ для «0» и «1», может быть устранено. Можно построить теорию, в которой рассматриваются также и все «асимметричные» случаи (Мартин-Лёф [10]).

---

[1]) И независимо от него Соломонов [18]. — *Прим. перев.*

§ 1. Сложность конечных 0-1-слов по Колмогорову

Мы начнем с идеи Колмогорова определять сложность конечного 0-1-слова $w = w_1 \ldots w_n \in \Omega$ минимальной длиной программы, которая необходима для того, чтобы некоторая машина Тьюринга напечатала w.

1.1. Определение. Пусть $A = A(*\,|\,*)$ есть некоторая вычислимая по Тьюрингу функция, сопоставляющая определенным парам (n, p) $(n = 0, 1, \ldots; p \in \Omega)$ конечные 0-1-слова $w = A(p\,|\,n)$, удовлетворяющие дополнительному условию $|w| = n$. Пусть для каждого конечного 0-1-слова w длины $|w| = n$ множество

$$P(w) = \{p \mid A(p\,|\,n) = w\}$$

есть совокупность всех программ, выполнение которых имеет своим результатом w. Назовем

$$K_A(w) = \inf_{p \in P(w)} |p|$$

сложностью (по Колмогорову) *w относительно A*. При этом, как обычно, положим $\inf \varnothing = \infty$ [1]).

Последнее соглашение означает, что слова, которые вообще не могут быть получены машиной, являются для нее бесконечно сложными.

Примеры. 1) Рассмотрим уже упомянувшуюся примитивную машину, печатающую для всех (n, p) только одни нули. Тогда

$$K_A(w) = \begin{cases} 0, & \text{если } w \text{ состоит из одних нулей,} \\ \infty & \text{в противном случае,} \end{cases}$$

так как, чтобы получить $w = 0 \ldots 0$, можно взять пустую программу $p = \square$, $|p| = 0$.

2) Рассмотрим «простую копирующую машину», описываемую соотношением

$$A(p\,|\,n) = p.$$

---

[1]) Точнее, $\inf_{p \in \varnothing} |p| = \infty$. — *Прим. перев.*

Естественно, что для нее

$$K_A(w) = |w|.$$

3) Рассмотрим «лексикографическую машину»: по данным (n, p) она печатает слово w длины n; при этом первые $[\log_2 n] + 1$ символов p она воспринимает как «число k единиц в слове w» (в двоичной записи), а оставшуюся часть p — как лексикографический номер слова w в множестве слов длины n, имеющих ровно k единиц. В связи с этим введем такое соглашение: когда число единиц больше n, будем говорить «одни единицы», в случае $\square$ (пустого множества) единиц будем говорить «ни одной единицы»; слово с лексикографическим номером $> \binom{n}{k}$ будем называть «лексикографически наибольшим среди слов, содержащих ровно k единиц», а слово с лексикографическим номером $\square$ — «лексикографически наименьшим среди слов, содержащих ровно k единиц». Введение таких соглашений необходимо потому, что при $n = 4$, например, число $[\log_2 n] + 1$ соответствует 7 единицам, т. е. тем самым количество единиц больше числа мест. Мы могли бы заменить их соответствующими ограничениями на «разумные» программы.

Если мы теперь будем вычислять, скажем, $K_A(010)$, то заметим сначала, что $n = 3$, значит, $[\log_2 n] + 1 = 2$, $k = 1$; поэтому первые 2 символа p должны быть равны 01 (двоичное представление для 1); лексикографическое упорядочение слов w с $|w| = 3$, содержащих ровно одну 1, имеет вид $100 < 010 < 001$ (0 предшествует 1, левое — правому); таким образом, p должно содержать по крайней мере еще один, третий символ, равный 1, так что $p = 011$ ($p = 0101$ или $p = 01001$ также дают $w = 010$). Тем самым мы получаем

$$K_A(010) = 3.$$

Наиболее важная ближайшая цель — освободиться от произвола в выборе машины, т. е. вычислимой по Тьюрингу функции $A = A(*|*)$. Если и не полностью, то хотя бы при асимптотическом подходе (при $n \to \infty$) эта цель может быть достигнута достаточно эффективно. Это обеспечивается следующей теоремой:

1.2. Теорема (Колмогоров [7]). *Существует вычислимая по Тьюрингу функция A вышеописанного вида, такая, что каждой другой рекурсивной функции $B(*|*)$ вышеописанного вида соответствует константа c_{AB}, для которой*

$$K_A(w) \leqslant K_B(w) + c_{AB} \qquad (w \in \Omega(\{0,1\})). \tag{1}$$

Замечание. Таким образом, c_{AB} может быть выбрана одной и той же для всех конечных 0-1-слов w. Функцию A с таким свойством мы называем *асимптотически оптимальной*[1]).

Доказательство. Напомним теорему Клини о перечислимости для вычислимых по Тьюрингу функций (см. часть III первой статьи, теорема 6.4): существует вычислимая по Тьюрингу функция

$$U' = U'(*|*|*):(m,\ n,\ p) \longrightarrow U'(p|n|m)$$

от трех переменных, такая, что функции $U'(*|*|m)$ пробегают все множество вычислимых по Тьюрингу функций от двух переменных (возможно, с повторениями), когда m пробегает множество всех натуральных чисел. Здесь, конечно, встречаются функции, которые не всегда удовлетворяют условию $|U'(p|n|m)| = n$. С интуитивной точки зрения очевидно, что соотношение

$$U(p|n|m) = \begin{cases} U'(p|n|m), & \text{когда } |U'(p|n|m)| = n, \\ \underbrace{0\ldots0}_{n} & \text{в противном случае} \end{cases}$$

снова определяет вычислимую по Тьюрингу функцию трех переменных, такую, что функции $U(*|*|m)$ пробегают (возможно, с повторениями) всю совокупность вычислимых по Тьюрингу функций описанного в определении 1.1 вида, когда m пробегает множество натуральных чисел.

---

[1]) Вот как разъясняет А. Н. Колмогоров в работе [19] смысл этой теоремы: существуют «универсальные» методы программирования A, обладающие свойством (1) и „...позволяющие программировать «что угодно» с длиной программы, которая превосходит длину при любом другом методе программирования не более чем на константу, зависящую лишь от этого второго метода программирования...". — *Прим. перев.*

Теперь мы зададим A, положив

$$A(p|n) = U(q|n|m),$$

где q и m получаются из p следующим образом:

a) машина A воспринимает только программы, для которых p имеет вид $p = m_1 m_1 \ldots m_r m_r 01q$, где $r > 0$, так что p начинается с последовательности пар нулей и(или) единиц, отделенных от остальной части q программы парой символов 01;

b) $m_1 \ldots m_r$ есть двоичная запись числа m.

Интуитивио ясно, что так определенная функция $A(*|*)$ вычислима по Тьюрингу; необходимо лишь сконструировать машину, которая расщепляет $p = m_1 m_1 \ldots$ $\ldots m_r m_r 01q$ иа пару слов $m_1 \ldots m_r = m$ и q, и соединить эту машину с $U(*|*|*)$. Мы удовлетворимся здесь этим пояснением.

Пусть теперь $B(*|*)$ есть произвольная вычислимая по Тьюрингу функция интересующего нас вида. Мы определим иомер m, для которого $B(*|*) = U(*|*|m)$; таких номеров может быть несколько, но нам достаточно иметь хотя бы одно такое m. Если слово w не может быть получеио машиной B, то $K_B(w) = \infty$ и (1) выполняется с любой константой c_{AB}. Мы можем, таким образом, выбирать эту константу, ориентируясь только иа те случаи, когда $K_B(w) < \infty$.

Пусть теперь w есть слово, которсе можно получить посредством B и для которого, например, $|w| = n$. Мы определим q так, чтобы

$$B(q|n) = w, \qquad |q| = K_B(w).$$

Рассмотрим теперь двоичную запись $m_1 \ldots m_r$ числа m и образуем воспринимаемую машиной A программу

$$p = m_1 m_1 \ldots m_r m_r 01q.$$

Для этой программы

$$A(p|n) = U(q|n|m) = B(q|n) = w,$$

причем

$$K_A(w) \leqslant |p| = 2r + 2 + |q| = 2r + 2 + K_B(w).$$

Таким образом, мы можем выбрать $c_{AB}=2r+2$, где r есть длина двоичной записи номера m для B в представлении U.

Интуитивно это сводится к следующему: A может все, что может B, если только A сообщен номер m для B в представлении U; при этом c_{AB} с точностью до некоторых деталей кодирования равно длине этого сообщения.

Соглашение. В дальнейшем мы зафиксируем некоторую асимптотически оптимальную вычислимую по Тьюрингу функцию A интересующего нас вида, положим

$$K(w)=K_A(w) \qquad (w \in \Omega)$$

и назовем $K(w)$ (просто) *сложностью слова* w.

Теорема 1.2 гарантирует нам, что при замене некоторой асимптотически оптимальной функции A на какую-то другую (A') $K(w)$ может измениться не более чем на $c_{AA'}+c_{A'A}$ и эта граница не зависит от w.

1.3. Теорема. *Для произвольных целых чисел $n>0$, $d\geqslant 0$ найдется по крайней мере*

$$2^n\left(1-\frac{1}{2^d}\right)$$

слов $w=w_1\ldots w_n$ длины n, для которых

$$K(w)\geqslant n-d.$$

В частности, положив $d=0$, мы получим, что всегда существуют слова w, для которых $K(w)\geqslant n$.

Доказательство. Пусть $a=n-d$. Соотношение $K(w)<c$ означает, что имеется программа p, для которой $|p|<a$ и $A(p|n)=w$. Подсчитаем теперь количество программ p длины $|p|<a$: имеется одна программа длины 0, а именно пустая программа $\square$; имеются две программы длины 1, а именно 0 и 1; имеется 2^k программ длины k; итак, всего

$$1+2+\ldots+2^{a-1}=\begin{cases} 0 & \text{при } a=0,\\ 2^a-1 & \text{при } a\geqslant 1.\end{cases}$$

В любом случае

$$1+2+2^2+\ldots+2^{a-1}<2^a \qquad (a=0,\ 1,\ 2,\ \ldots),$$

так что имеется не более 2^a слов $w=w_1\ldots w_n$ с $K(w)<a$. Так как общее число слов длины n равно 2^n, то найдется не менее $2^n-2^a=2^n-2^{n-d}=2^n\left(1-\frac{1}{2^d}\right)$ слов w длины n с $K(w)\geqslant n-d$.

Мы займемся теперь следующим вопросом: насколько сложными могут быть слова, которые машина печатает сама по себе?

Ситуация, сложившаяся в итоге предшествующих рассмотрений, такова: в нашем распоряжении имеется универсальная машина A, которая печатает любое желаемое конечное 0-1-слово w, если только ей сообщена верная программа. В худшем случае это выглядит так: имеется машина B (весьма ограниченная по своим возможностям), которая может печатать одно-единственное слово w; когда мы сообщаем машине A только «номер» m этой машины, A работает, как B, и тоже печатает w. Итак, машина A обладает фантастическими возможностями, но непродуктивным интеллектом — ей необходимо точно указать, задав n и p, что она должна делать.

Теперь нас интересует такой вопрос: рассмотрим машину, которая не снабжается меняющимися программами, а предоставлена самой себе, т. е. применяется к пустой ленте и печатает бесконечную последовательность $w^{(0)}$, $w^{(1)}$, ... 0-1-слов длины 0, 1, ...; как обстоит дело со сложностью $K(w^{(0)})$, $K(w^{(1)})$, ...?

Математическая реализация такой машины — это некоторая вычислимая по Тьюрингу функция F, которая сопоставляет каждому целому числу $n\geqslant 0$ некоторое 0-1-слово $w^{(n)}=w_1^{(n)}\ldots w_n^{(n)}=F(n)$ длины n. Теперь очень легко ответить на наш вопрос: определим машину $B(*|*)$ вышеописанного вида, положив

$$B(p|n)=F(n).$$

Тогда, согласно теореме 1.2, найдется константа c_{AB}, для которой

$$K(w)=K_A(w)\leqslant K_B(w)+c_{AB} \qquad (w\in\Omega(\{0,\ 1\})).$$

Но $K_B(w^{(n)})=0$, так как при заданной длине n слова в качестве программы p можно выбрать, например, пустую программу $p=\square$, для которой $B(p|n)=B(\square|n)=F(n)=w^{(n)}$. Следовательно,

$$K(w^{(n)})\leqslant c_{AB}$$

и справедлива такая теорема:

1.4. Теорема. *Любая машина, предоставленная самой себе, печатает только* 0-1-*слова ограниченной сложности.*

Если мы вспомним первоначальную идею Колмогорова [7] определять случайные слова как слова большой сложности (для данного n), то содержание теоремы 1.3 можно выразить так: «существуют случайные слова», а содержание теоремы 1.4 так: «машина не может самостоятельно печатать случайные слова произвольной длины».

§ 2. *Один неудавшийся подход*

Мы хотим попытаться использовать меру сложности по Колмогорову *конечных слов* для определения случайности *бесконечных* 0-1-последовательностей. Этой цели служит следующее грубое определение:

2.1. Определение. Бесконечная 0-1-последовательность $x=x_1x_2\ \ldots$ называется *квазислучайной*, если существует постоянная $c=c(x)$, для которой

$$K(x_1\ldots x_n)\geqslant n-c \qquad (n=1,\ 2,\ \ldots).$$

Мы докажем теперь одно утверждение, из которого следует, что идея, воплощенная в этом определении, еще не вполне пригодна: *в каждой бесконечной* 0-1-*последовательности* $x_1\ x_2\ \ldots$ *значение сложности* $K(x_1\ldots x_n)$ *бесконечно много раз становится значительно меньше* n, *т. е. имеется бесконечно много отрезков с высокой упорядоченностью.* В связи с этим нам придется еще раз пересмотреть определение понятия «случайная бесконечная 0-1-последовательность», но уже с новой точки зрения (§ 4).

2.2. Теорема (Мартин-Лёф [9]). *Пусть* $f(n)$ $(n=1,\ 2,\ \ldots)$ *есть некоторая вычислимая по Тьюрингу функция* *со значениями во множестве* $\{0, 1, \ldots\}$, *такая, что*

(1) $$\sum_{n=1}^{\infty} \frac{1}{2^{f(n)}} = \infty$$

(т. е. $f(n)$ становится «очень часто слишком большой»). *Тогда для каждой бесконечной* 0-1-*последовательности* $x_1 x_2 \ldots$ *найдется бесконечно много* n, *для которых выполняется неравенство*

(2) $$K(x_1 \ldots x_n) < n - f(n).$$

Замечание. Если $f(n)$ бесконечно много раз принимает малые значения, то может случиться, что (2) выполняется как раз для этих значений n, и в этом случае (2) имеет относительно небольшую ценность. Напротив, если мы возьмем, например, вычислимую по Тьюрингу функцию

$$f(n) = [\log_2 n],$$

то получнм

$$\sum_{n=1}^{N} \frac{1}{2^{f(n)}} \geqslant \frac{1}{2} \sum_{n=1}^{N} \frac{1}{n} \to \infty,$$

н теорема утверждает, что бесконечно много раз

$$K(x_1 \ldots x_n) < n + 1 - \log_2 n.$$

Отсюда немедленно следует

2.3. Теорема. *Не существует квазислучайных* 0-1-*последовательностей.*

Эта теорема свидетельствует о том, что определение 2.1 неудачно.

Доказательство теоремы 2.2. 1) Из технических соображений мы временно заменим $f(n)$ большей функцией, а именно вычислимой по Тьюрингу функцией $g(n)$ $(n = 1, 2, \ldots)$, для которой

(3) $$\sum_{n=1}^{\infty} \frac{1}{2^{g(n)}} = \infty,$$

(4) $$g(n) - f(n) \to \infty.$$

Для этого мы разобьем ряд 1, 2, ... с помощью подпоследовательности $0=m_0<m_1<\ldots$ на отрезки таким образом, чтобы

$$\sum_{n=1}^{m_1}\frac{1}{2^{f(n)}}>2^0=1,\quad \sum_{n=m_1+1}^{m_2}\frac{1}{2^{f(n)}}>2^1,\ \ldots,$$

т. е.

$$\sum_{n=m_k+1}^{m_{k+1}}\frac{1}{2^{f(n)}}>2^k\quad (k=0,\ 1,\ \ldots), \tag{5}$$

и положим

$$g(n)=f(n)+k\qquad (m_k<n\leqslant m_{k+1},\ k=0,\ 1,\ \ldots). \tag{6}$$

Здесь (5) выполняется в силу (1), а (4) следует из (6). Однако (3) также имеет место, поскольку

$$\sum_{n=1}^{\infty}\frac{1}{2^{g(n)}}=\sum_{k=0}^{\infty}\sum_{m_k<n\leqslant m_{k+1}}\frac{1}{2^{f(n)+k}}>$$

$$>\sum_{k=0}^{\infty}\frac{1}{2^k}\sum_{m_k<n\leqslant m_{k+1}}\frac{1}{2^{f(n)}}>\sum_{k=0}^{\infty}\frac{2^k}{2^k}=\infty.$$

Интуитивно ясно, что подходящая машина может обеспечить нахождение чисел m_0; m_1, ... и тем самым значений $g(1)$, $g(2)$, ..., если с ней нужным образом соединена машина, вычисляющая $f(1)$, $f(2)$, ... Таким образом, $g(n)$ $(n=1,\ 2,\ \ldots)$ снова есть вычислимая по Тьюрингу функция.

2) Мы используем идею, высказанную еще Борелем [3] ((с другими целями) приближения действительных чисел рациональными), чтобы построить машину B, которая порождает бесконечно много чисел n, удовлетворяющих неравенству

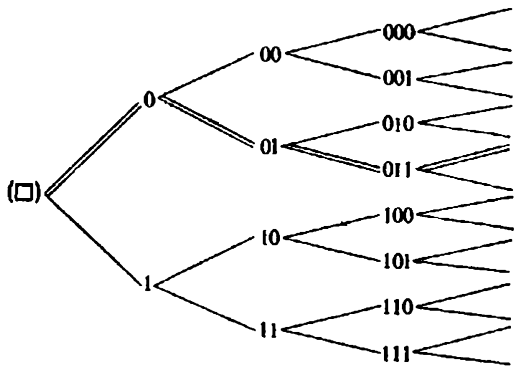
$$K_B(x_1\ldots x_n)<n-g(n).$$

Согласно теореме 1.2, существует константа $c>0$, для которой

$$K(x_1\ldots x_n)<n-g(n)+c.$$

В силу (4) отсюда следует требуемое неравенство (2).

Конструкция B использует упорядочение всех конечных 0-1-слов: a) по длине n слова, b) при фиксированном n — лексикографическое упорядочение; можно представлять себе, например, следующую диаграмму:



в которой n-й столбец, читаемый сверху вниз, содержит лексикографически упорядоченную совокупность всех 0-1-слов длины n и от каждого слова отходят вправо две соединяющие линии к двум возможным продолжениям слова, получаемым добавлением следующего символа (0 или 1). Наша исходная 0-1-последовательность $x_1 x_2 \ldots$ может быть описана как последовательностью $x_1 \ldots x_n$ $(n = 1, 2, \ldots)$ ее начальных отрезков, так и соответствующим этой последовательности «путем» на диаграмме, идущим вдоль соединительных линий. Мы обозначили на рисунке начало этого пути для последовательности 01111001... двойной линией.

В каждом столбце (с номером $n = 1, 2, \ldots$) этой схемы мы выделим некоторое подмножество M_n, причем так, чтобы

$$M_n = \varnothing$$

всякий раз, когда $n - g(n) < 0$. Интересен процесс поэтапного построения множеств M_n при $n - g(n) \geqslant 0$. Ввиду (3) этот случай должен встречаться бесконечно много раз, и мы можем вычислить посредством некоторой машины Тьюринга все члены последовательности $n = n_1$, n_2, ... чисел, для которых он имеет место; действительно, функция $g(n)$ $(n=1, 2, \ldots)$ вычислима по Тьюрингу, т. е. множество пар $(n, g(n))$ $(n=1, 2, \ldots)$ перечислимо по Тьюрингу.

Мы начнем с равенств $M_1=\ldots=M_{n_1-1}=\varnothing$, пока впервые не наступит случай $n_1-g(n_1)\geqslant 0$. Тогда в качестве элементов M_{n_1} мы возьмем $2^{n_1-g(n_1)}$ верхних слов n_1-го столбца (они являются лексикографически наименьшими). Теперь мы временно блокируем все пути, идущие направо от элементов M_{n_1}, и положим $M_{n_1+1}=\varnothing, \ldots$, пока не получим опять $n=n_2$ с $n_2-g(n_2)\geqslant 0$. Находящиеся на блокированных путях верхние слова длины n_2 общим числом $2^{n_2-n_1}\cdot 2^{n_1-g(n_1)}=2^{n_2-g(n_1)}$ мы *не включим* в множество M_{n_2}, а образуем это множество из непосредственно примыкающих к ним $2^{n_2-g(n_2)}$ слов, одновременно блокируя также и все пути, которые ведут из элементов этого множества направо. Когда, продолжая таким образом, мы придем к n_k, т. е. k-му числу n, для которого $n-g(n)\geqslant 0$, верхние $2^{n_k}\left(\frac{1}{2^{g(n_1)}}+\ldots+\frac{1}{2^{g(n_{k-1})}}\right)$ элементов n_k-го столбца будут находиться на уже блокированных путях. Заметим теперь, что, согласно (3),

$$\sum_{n_k-g(n_k)\geqslant 0}\frac{1}{2^{g(n_k)}}\geqslant\sum_{n=1}^{\infty}\frac{1}{2^{g(n)}}-\sum_{n=1}^{\infty}\frac{1}{2^n}=\sum_{n=1}^{\infty}\frac{1}{2^{g(n)}}-1=\infty,$$

ввиду чего неизбежно через какое-то число шагов будут блокированы более $2^{n_k}-2^{n_k-g(n_k)}$ слов столбца n_k, так что выбор $2^{n_k-g(n_k)}$ слов для M_{n_k} будет невозможен. Как только это впервые произойдет—этот момент также вычислим по Тьюрингу,—мы просто присоединим к элементам M_{n_k} все еще не блокированные слова, отменим блокировки и начнем все сначала для (n_k+1)-го столбца: полагаем $M_n=\varnothing$ для всех $n=n_k+1, \ldots$, пока не получим неравенство $n_{k+1}-g(n_{k+1})\geqslant 0$, и т. д.

Из соотношения (3) следует, что мы должны будем начинать так бесконечно много раз. Этот *пульсирующий процесс* может быть, конечно, реализован некоторой машиной.

Теперь перенумеруем элементы M_n в лексикографическом порядке, начиная с нулевого элемента сверху и до $2^{n-g(n)}$-го элемента сверху, а затем выпишем полученные номера в двоичной форме: $0=0$, $1=1$, $2=10$, $\ldots$. Возникнет последовательность $a^{(0)}, \ldots, a^{(r_n-1)}$ 0-1-номеров, длины которых не превышают $n-g(n)$. Соотношение

$$B(p\,|\,n) = \text{слово с номером } j \text{ в } M_n, \text{ если } p = a^{(j)},$$

определяет машину Тьюринга, описанную в определении 1.1.

Рассмотрим теперь бесконечную последовательность $x_1 x_2 \ldots$ и вычислим для построенной нами машины B значение сложности $K_B(x_1 \ldots x_n)$. Ввиду того что вышеописанный пульсирующий процесс постоянно повторяется с самого начала, будет бесконечно часто повторяться и включение $x_1 \ldots x_{n_k} \in M_{n_k}$ и тем самым будет выполняться соотношение

$$K_B(x_1 \ldots x_{n_k}) \leqslant n_k - g(n_k),$$

как и утверждалось.

§ 3. *Пространство бесконечных 0-1-последовательностей*

Прежде чем дать окончательный ответ на вопрос о том, как нужно определять понятие случайной бесконечной 0-1-последовательности, мы оставим на некоторое время царство вычислений по Тьюрингу и займемся изучением множества

$$X = \{x = x_1 x_2 \ldots \,|\, x_1, x_2, \ldots = 0 \text{ или } 1\}$$

всех бесконечных 0-1-последовательностей в беззаботно-классическом смысле, а именно с точки зрения топологии и теории меры. Полученные здесь результаты мы частично вновь переформулируем для множества

$$\Omega = \{w = w_1 \ldots w_n \,|\, w_1, \ldots, w_n = 0 \text{ или } 1\} \qquad (\ni \square)$$

всех конечных 0-1-слов и свяжем их с результатами по Тьюрингу. Позже, однако, нам также понадобятся определенные результаты, довольно типичным образом выпадающие из царства Тьюринга.

В X определяется *метрика* $|x, y| = \sum_{t=1}^{\infty} |x_t - y_t| \cdot 2^{-t}$ $(x = x_0 x_1 \ldots,\ y = y_0 y_1 \ldots \in X)$; легко проверяются соотношения

1) $|x, y| \geqslant 0$, причем $|x, y| = 0$ тогда и только тогда, когда $x = y$;
2) $|x, z| \leqslant |x, y| + |y, z| \quad (x, y, z \in X)$.

Таким образом, x и y находятся в этой метрике тем ближе друг к другу, чем в большем числе компонент они совпадают. Для последовательности $x^{(1)}, x^{(2)}, \ldots \in X$ утверждение о сходимости по метрике $|x^{(k)}, x| \to 0$ к элементу $x \in X$ равносильно высказыванию: для любого $t_0 > 0$ найдется такое $k_0 > 0$, что для всех $k \geqslant k_0$

$$x_1^{(k)} = x_1, \ \ldots, \ x_{t_0}^{(k)} = x_{t_0}$$

(совпадение всех компонент с номерами $1, \ldots, t_0$). Ввиду этого очень просто из произвольной заданной в X последовательности $x^{(1)}, x^{(2)}, \ldots$ выбрать с помощью диагонального процесса некоторую сходящуюся по метрике подпоследовательность.

Действительно, в 0-1-последовательности $x_1^{(1)}, x_1^{(2)}, \ldots$ первых компонент последовательностей $x^{(k)}$ хотя бы одно из значений 0, 1 встречается бесконечно часто. Для подходящих $1 \leqslant k_{11} \leqslant k_{12} \leqslant \ldots$ выполняются равенства $x_1^{(k_{10})} = x_1^{(k_{11})} = \ldots$.

Теперь рассмотрим вторые компоненты этой подпоследовательности: в последовательности $x_2^{(k_{11})}, x_2^{(k_{12})}, \ldots$ имеется подпоследовательность $x_2^{(k_{21})} = x_2^{(k_{22})} = \ldots$. Действуя в том же духе и дальше, положим в конце концов $x = x_0^{(k_{11})} x_1^{(k_{22})} \ldots$ и при $\nu \to \infty$ получим $|x^{(k_{\nu\nu})}, x| \to 0$. Итак, X (с метрикой $|\cdot, \cdot|$) есть компактное пространство — метрический компакт.

Если у читателя после этого возникло ощущение, что X — почти самый простой метрический компакт на свете, то он совершенно прав, и я прошу его сохранять это ощущение также и перед лицом, возможно, довольно странного на первый взгляд факта, что для каждого конечного 0-1-слова $w = w_1 \ldots w_n$ так называемое *цилиндрическое множество*

$$[w] = [w_1 \ldots w_n] = \{x = x_1 x_2 \ldots \mid x_1 = w_1, \ldots, x_n = w_n\} = \\ = \{x = w_1 \ldots w_n x_{n+1} \ldots \mid x_{n+1}, x_{n+2}, \ldots = 0, 1\}$$

(при этом, конечно, полагают $[\square]=X$) является одновременно и замкнутым, и открытым. В самом деле,

a) если $x\in[w]$ и $|x, y|<2^{-n}$, то $y_1=x_1=w_1, \ldots, y_n=$ $=x_n=w_n$, так что $y\in[w]$, т. е. $[w]$ открыто;

b) из соотношения

$$X=\sum_{w_1, \ldots, w_i=0,1}[w_1 \ldots w_n]$$

(где $\sum$ означает объединение непересекающихся множеств) следует также, что

$$[w]=X\diagdown\sum_{\substack{v_1, \ldots, v_n=0,1 \\ v_1 \ldots v_n\neq w_1 \ldots w_n}}[v_1 \ldots v_n],$$

и $[w]$ как дополнение открытого множества должно быть также и замкнутым.

Для каждого $x=x_1x_2\ldots\in X$ цилиндр $[x_1 \ldots x_n]$ является, очевидно, открытым множеством диаметра 2^{-n}, содержащим x. Последовательность $[x_1], [x_1 x_2], \ldots$ этих множеств образует базис окрестностей x в метрической топологии.

Мы хотим ввести в X не только (метрическую) *топологию*, ио также и *вероятностную структуру*. Мы достигнем этого, сопоставив каждому цилиндрическому множеству $[w_1 \ldots w_n]$ вероятность $p([w_1 \ldots w_n])=2^{-n}$, а затем каждому миожеству $M\subseteq X$, являющемуся объединением конечного числа попарно иепересекающнхся цилиндрическнх множеств, $M=[w^{(1)}]+\ldots+[w^{(r)}]$ (слова $w^{(i)}$ могут иметь разную длину), вероятность $p(M)=p([w^{(1)}])+\ldots+p([w^{(r)}])$. Отсюда, в частиости, следует, что $p(X)=1$. Вообще же $0\leqslant p(M)\leqslant 1$. В связи с этим необходимо, конечно, выяснить, не возникнут ли из различных представлений $M=[w^{(1)}]+\ldots+[w^{(r)}]=[v^{(1)}]+\ldots+[v^{(s)}]$ различные значения меры $p([w^{(1)}])+\ldots+p([w^{(r)}])\neq p([v^{(1)}])+\ldots$ $\ldots+p([v^{(s)}])$; эту задачу легко свести к ситуации $M=$ $=[w_1 \ldots w_n]=[w_1 \ldots w_n 0]+[w_1 \ldots w_n 1]$, в которой наши сомнения устраняет равенство $\frac{1}{2^n}=\frac{1}{2^{n+1}}+\frac{1}{2^{n+1}}$. Те, кому уже приходилось когда-либо иметь дело с теорией вероятностей и теорией меры, знают, что иельзя останавливаться на определении $p(M)$ для названных простых по строению множеств M и следует расширить область определения p.

Нам понадобятся здесь только обобщение на *открытые множества* и определение *нулевого множества*. Все это можно осуществить без особых усилий. Пусть $U \subseteq X$ открыто и U_1 есть объединение всех содержащихся в U цилиндрических множеств «длины» 1 (т. е. $U_1 = \varnothing$, $[0]$, $[1]$ или $= X = [0] + [1]$). Так как U_1 есть конечное объединение замкнутых множеств — не более 2^1 таких цилиндрических множеств — и все они замкнуты, то U_1 само замкнуто и $U \setminus U_1$ открыто. Очевидно, что $U \setminus U_1$ больше не содержит непустых цилиндрических множеств «длины» 1. Пусть U_2 есть объединение всех (максимум 2^2) содержащихся в $U \setminus U_1$ цилиндрических множеств «длины» 2 (так что $U_2 = \varnothing$, $[00]$, $[01]$, $[10]$, $[11]$, $[00]+[11]$, $[00]+[10]$ или $[11]+[01]$. Очевидно, что $U_1 \cap U_2 = \varnothing$ и $U \setminus (U_1 + U_2)$ открыто. Так строятся одно за другим попарно непересекающиеся подмножества $U_1, U_2, \ldots$ множества U. Их объединение есть U: пусть $x = x_1 x_2 \ldots \in U$ и n — минимальное из чисел, удовлетворяющих соотношению $[x_1 \ldots x_n] \subseteq U$; тогда $x \in U_n$. Величины $p(U_1)$, $p(U_2), \ldots$, очевидно, уже определены, и ввиду неравенства $p(U_1) + \ldots$ $\ldots + p(U_n) = p(U_1 + \ldots + U_n) \leqslant p(X) = 1$ ряд $p(U_1) +$ $+ p(U_2) + \ldots$ сходится к пределу $\lim\limits_{n \to \infty} p(U_1 + \ldots + U_n) \leqslant 1$. Значение суммы этого ряда мы принимаем за вероятность $p(U)$ множества U. Если $M \subseteq X$ и для каждого $\varepsilon > 0$ найдется открытое U, $M \subseteq U \subseteq X$, для которого $p(U) < \varepsilon$, то мы называем M *нулевым множеством* и пишем $p(M) = 0$, $p(X \setminus M) = 1$. При этом имеет место такое утверждение:

Дополнение $X \setminus M$ нулевого множества непусто; более того, оно несчетно и метрически плотно в X.

Сначала мы докажем следующее:

1) Если U открыто и каждое из множеств $U'_1 \subseteq U'_2 \subseteq \ldots$ $\ldots \subseteq U$ допускает представление в виде конечного объединения цилиндрических множеств, причем $U'_1 \cup U'_2 \cup \ldots = U$, то $\lim p(U'_n) = p(U)$. Действительно, каждому k соответствует n, для которого $U_1 + \ldots + U_k \subseteq U'_n$, так как в противном случае все замкнутые множества $(U_1 + \ldots$ $\ldots + U_k) \setminus U'_n$ были бы непусты и ввиду компактности имело бы место противоречивое соотношение

$$\varnothing \neq \bigcap_n (U_1 + \ldots + U_k) \setminus U'_n = (U_1 + \ldots + U_k) \setminus \bigcup_n U'_n =$$
$$= (U_1 + \ldots + U_k) \setminus U = \varnothing;$$

но из $U_1+\ldots+U_k\subseteq U'_n$ следует, что $p(U_1+\ldots+U_k)\leqslant\leqslant p(U'_n)$; таким образом, мы получаем неравенство $p(U)\leqslant\lim p(U'_n)$; аналогичные рассуждеиия, но с заменой знака $\leqslant$ на знак $\geqslant$ дают нам требуемое равенство.

2) Если U, V — открытые множества, то $U\cup V$ открыто и $p(U\cup V)\leqslant p(U)+p(V)$. Мы находим множества U'_1, V'_1, U'_2, V'_2, ... описанного в п. 1) вида, удовлетворяющие соотношеииям $U'_1\subseteq U'_2\subseteq\ldots\subseteq\bigcup U'_n=U$, $V'_1\subseteq V'_2\subseteq\ldots\ldots\subseteq\bigcup V'_n=V$, и замечаем, что множества $U'_1\cup V'_1\subseteq\subseteq U'_2\cup V'_2\subseteq\ldots$ представимы в виде объедииений коиечного числа попарно непересекающихся цилиндрических множеств и $U\cup V=\bigcup\limits_n(U'_n\cup V'_n)$, так что $p(U\cup V)=\lim p(U'_n\cup V'_n)\leqslant\leqslant\lim p(U'_n)+\lim p(V'_n)=p(U)+p(V)$. Нераввнство следует из оценки $p(U'_n\cup V'_n)\leqslant p(U'_n)+p(V'_n)$, которую совсем нетрудно получить, если представить U'_n, V'_n и $U'_n\cup V'_n$ в виде объедииений попарно непересекающихся цилиндрических множеств $[\omega_1\ldots\omega_r]$ одной и той же «длины» r; возможно, что некоторые из слагаемых 2^{-r}, учтенные в $p(U'_n\cup V'_n)$ только один раз, входят в сумму $p(U'_n)+p(V'_n)$ дважды.

3) Если U_1, U_2, ... — открытые множества, то множество $U_1\cup U_2\cup\ldots$ также открыто и $p(U_1\cup U_2\cup\ldots)\leqslant\leqslant p(U_1)+p(U_2)+\ldots$. Чтобы доказать это, следует выбрать для каждого n возрастающую последовательиость $U'_{n1}\subseteq U'_{n2}\subseteq\ldots$ подмножеств U_n, каждое из которых допускает представление в виде конечного объединения цилиндрических множеств и при этом выполнено соотношеиие $U_n=U'_{n1}\cup U'_{n2}\cup\ldots$. Тогда и миожества $U'_k==U'_{1k}\cup\ldots\cup U'_{kk}$ являются конечными объединениями цилиндрических множеств, причем выполняются соотношения $U'_1\subseteq U'_2\subseteq\ldots$, $U'_1\cup U'_2\cup\ldots=U_1\cup U_2\cup\ldots$. Мы заключаем из 1) и 2), что $p(U_1\cup U_2\cup\ldots)=\lim\limits_{k\to\infty}p(U'_k)\leqslant\leqslant\lim\limits_{k\to\infty}[p(U'_{1k})+\ldots+p(U'_{kk})]\leqslant p(U_1)+p(U_2)+\ldots$.

4) Если $M(\subseteq X)$ — счетное множество, то M есть нулевое множество: для даиного $\varepsilon>0$ выберем числа n_1, n_2, ... так, чтобы $\frac{1}{2^{n_1}}+\frac{1}{2^{n_2}}+\ldots<\varepsilon$. Пусть $M==\{x^{(1)}, x^{(2)}, \ldots\}$. Положим $\tilde U_1=[x_1^{(1)}\ldots x_{n_1}^{(1)}]$, $\tilde U_2=[x_1^{(2)}\ldots\ldots x_{n_2}^{(2)}]$, ... и положим $U'_n=\tilde U_1\cup\ldots\cup\tilde U_n$, $U=\tilde U_1\cup\tilde U_2\cup\ldots$.

Очевидно, имеют место неравенства $\lim\limits_{n\to\infty} p(U_n') \leqslant \frac{1}{2^{n_1}} + \frac{1}{2^{n_2}} + \ldots < \varepsilon$ и тем самым $p(U) < \varepsilon$. Но при этом $M \subseteq U$.

Теперь мы можем доказать наш результат. Если бы $X \setminus M$ было счетным, то каждому $\varepsilon > 0$ соответствовали бы открытые множества U, V, для которых $M \subseteq U$, $X \setminus M \subseteq V$, $p(U) < \varepsilon/2$, $p(V) < \varepsilon/2$ (здесь воспользуемся 3) в применении к $X \setminus M$). Следовательно, $X = U \cup V$, так что $1 = p(X) \leqslant p(U) + p(V) < \varepsilon/2 + \varepsilon/2 = \varepsilon$, и при $\varepsilon < 1$ мы имеем противоречие. Итак, $X \setminus M$ — несчетное множество. Повторив это рассуждение (с $\varepsilon < 1/2^{n+1}$) в применении к произвольному цилиндрическому множеству $[w_1 \ldots w_n]$, мы увидим, что даже $[w] \setminus M$ несчетно и, в частности, $X \setminus M$ метрически плотно в X.

Мы хотим использовать идеи, развитые нами во время этой экскурсии в не слишком подходящее для вычислений по Тьюрингу пространство X, для некоторых построений в привычном множестве Ω всех конечных 0-1-слов, для чего мы постоянно будем использовать соответствие

$$w \leftrightarrow [w]$$

между элементами Ω и подмножествами X. Мы можем еще расширить это соответствие: каждому подмножеству $U \subset X$ мы сопоставим множество всех тех w, для которых $[w] \subseteq U$, т. е. подмножество $W = W(U) \subset \Omega$. Как можно охарактеризовать полученные таким образом подмножества $W \subset \Omega$? Пусть $v = w_1 \ldots w_r v_{r+1} \ldots v_s$ есть некоторое продолжение $w = w_1 \ldots w_r$; тогда $[v] \subseteq [w]$ и из включения $[w] \subseteq U$ следует включение $[v] \subseteq U$, так что из $w \in W$ следует $v \in W$. Всякое множество $W \subseteq \Omega$, содержащее вместе с каждым словом все его продолжения, мы назовем *секвенциальным*. Справедливо утверждение: множества вида $W = W(U)$ $(U \subseteq X)$ и только они являются секвенциальными множествами. Выше мы уже показали, что каждое множество $W = W(U)$ секвенциально. Нам осталось показать, что каждое секвенциальное множество $W \subseteq \Omega$ имеет вид $W = W(U)$ (для соответствующего $U \subset X$). Чтобы доказать это, положим для данного секвенциального $W \subseteq \Omega$

$$U = \bigcup_{w \in W} [w].$$

Тогда легко проверяется, что $W = W(U)$. Непосредственно видно, что это множество U открыто как объединение открытых множеств; если ограничиться *открытыми* подмножествами $U \subseteq X$, то соответствие $W = W(U) \leftrightarrow U$ является взаимно однозначным, т. е. открытые подмножества $U \subset X$ и секвенциальные подмножества $W \subset \Omega$ — это лишь две стороны одного и того же явления. Мы обозначим открытое подмножество $U \subset X$, сопоставляемое таким образом секвенциальному подмножеству $W \subset \Omega$, через $U = [W]$, так что $W = W([W])$, $U = [W(U)]$.

Чтобы сразу указать серьезное применение этого отождествления, мы определим теперь также и для секвенциальных подмножеств $W \subset \Omega$ вероятность

$$p(W) = p([W]).$$

Выясните в виде упражнения, как вычислить $p(W)$, не переходя к $[W]$.

§ 4. *Случайные бесконечные 0-1-последовательности*

Теперь в наших руках находятся все средства для того, чтобы разумиым образом определить, когда бесконечная 0-1-последовательность $x = x_1 x_2 \ldots$ должна называться случайной.

В чем, собственно, была наша ошибка в первой неудачной попытке, о которой рассказывалось в § 2? Мы попробовали дать определение

$$x \text{ квазислучайна} \Leftrightarrow K(x_1 \ldots x_n) \geqslant n - c \qquad (n = 1,\ 2,\ \ldots)$$

и были вынуждены признать, что квазислучайных 0-1-последовательностей не существует (теорема 2.2). Мартин-Лёф [9,10] предложил называть 0-1-последовательности случайными, если они выдерживают так называемый универсальный секвенциальный тест. Этот подход себя оправдал (ср. также модификацию Шнорра [13]), и мы хотим здесь о нем рассказать.

Тестом называют испытание, которому подвергается испытуемый объект и которое он либо выдерживает, либо нет. Рассмотрим следующее испытание: предлагается анкета, в которой нужно для каждого вопроса отметить крестиком правильный ответ; затем анкета сверяется с шаблоном, и если в ней встречается более двух ошибок, то она отбраковывается. Это можно описать, скажем, так: имеется n вопросов и для каждого вопроса три клеточки для крестиков, так что всего 3^n возможностей заполнить анкету; лишь одна из этих возможностей безошибочна, ровно $2n$ содержат по одной ошибке и ровно $4n(n-1)$ содержат по две ошибки. Остальные $3^n-2n-4n(n-1)=$ $=3^n-4n^2+2n$ возможностей соответствуют неудачному исходу и образуют так называемую «критическую область» теста. Если анкета заполняется совершенно случайно с одинаковыми вероятностями для всех возможностей, то исход неудачен с «гарантирующей вероятностью» $(3^n-4n^2+2n)/3^n=1-(4n^2-2n)/3^n$. Так как 3^n возрастает с ростом n гораздо быстрее, чем $4n^2-2n$, то этот метод заполнения анкеты для больших n рекомендуется ещё в меньшей степени, чем для $n=1$, где вероятность неудачного исхода равна все же только $^2/_3$.

Если мы теперь снова вернемся к 0-1-словам и будем работать какое-то время со словами фиксированной длины $n\geqslant 1$, то под *тестом*, говоря математическим языком, мы будем просто понимать подмножество K (также называемое критической областью теста) множества $\{0,1\}^n$ всех 0-1-слов длины n, а под «гарантирующей вероятностью» — величину $2^{-n}\cdot|K|$, где $|K|$ — число элементов K.

Ввиду того что в наших рассмотрениях встречаются 0-1-слова самых различных длин, стоит допустить в качестве критических областей подмножества множества Ω *всех* конечных 0-1-слов. Дальше мы будем одновременно рассматривать различные значения «гарантирующей вероятности» (наиболее удобны для нас $1=2^{-0}, 2^{-1}, 2^{-2}, \ldots$), и, наконец, все наши процедуры должны быть рекурсивны, т. е. вычислимы по Тьюрингу. Так мы приходим к существенному для последующего определению 4.1.

При этом мы будем постоянно переходить, пользуясь развитым в конце § 3 методом, от множества Ω всех конечных 0-1-слов ω к множеству X всех бесконечных 0-1-последовательностей x и от X к Ω и, в частности, будем говорить о вероятностях секвенциальных подмножеств Ω.

4.1. Определение. Перечислимое по Тьюрингу множество K упорядоченных пар

$$(m,\ w) \qquad (m \geqslant 0 — \text{целое},\ w \in \Omega)$$

называется *секвенциальным тестом*, если множества

$$K_m = \{w \mid w \in \Omega,\ (m,\ w) \in K\} \qquad (m = 0,\ 1,\ \ldots)$$

(его «критические области») удовлетворяют следующим условиям:

1) $K_0 \supseteq K_1 \supseteq \ldots$,
2) K_m секвенциально в смысле § 3 $(m = 0,\ 1,\ \ldots)$,
3) $p(K_m) \leqslant 2^{-m} \qquad (m = 0,\ 1,\ \ldots)$.

Требования 1)—3), если их переформулировать для пространства X всех бесконечных 0-1-последовательностей, означают следующее: имеется убывающая последовательность открытых подмножеств $[K_0] \supseteq [K_1] \supseteq \ldots$ пространства X, вероятности которых удовлетворяют неравенствам $p([K_m]) \leqslant 2^{-m}$ $(m = 0,\ 1,\ \ldots)$ и, таким образом, стремятся к нулю. В частности, множество

$$M = M_K = \bigcap_{m \geqslant 0} [K_m]$$

является *нулевым множеством*. Мы назовем его *нулевым множеством теста* K; оно состоит, нестрого говоря, из таких последовательностей $x = x_1x_2 \ldots$, которые не выдерживают теста K.

4.2. Теорема. *Существует секвенциальный тест U, такой, что любой секвенциальный тест K удовлетворяет включению*

$$K_{m+c} \subseteq U_m \tag{1}$$

с некоторой константой $c = c_{UK}$. Каждый такой тест U будет называться универсальным секвенциальным тестом. Если V — какой-нибудь другой универсальный секвенциальный тест, то $M_U = M_V$. Мы назовем нулевое множество $M \subseteq X$, однозначно определяемое равенством $M = M_U$ (U — универсальный секвенциальный тест), универсальным нулевым множеством, а элементы x множества $X \setminus M$ назовем случайными бесконечными 0-1-последовательностями.

Итак, M есть множество всех «универсально выживающих» последовательностей. *Последовательность слу-*

чайна, если она выдерживает некоторый универсальный тест, или, что ввиду (1) одно и то же, *если она выдерживает любой секвенциальный тест.* Согласно § 4, имеется несчетное множество случайных 0-1-последовательностей, и они плотны в X. Заметим, что этот результат не следует из одной лишь теории машин Тьюринга.

Доказательство. Мы начнем так же, как и при доказательстве теоремы 1.2. Согласно теореме о перечислимости (см. статью о перечислимости в этой книге, теорема 3.9), существует перечислимое по Тьюрингу подмножество T упорядоченных троек (k, m, w) $(k, m=0, 1, \ldots;$ $w \in \Omega)$, такое, что каждому секвенциальному тесту K соответствует по крайней мере одно значение k, для которого

$$K_m = \{w \mid (k, m, w) \in T\} \qquad (m=0, 1, \ldots).$$

Небольшая модификация позволит нам далее считать, что для любого k множество $\{(m, w) \mid (k, m, w) \in T\}$ является секвенциальным тестом. Пусть теперь U есть множество всех пар (m, w), для каждой из которых $(k, m+k+1, w) \in T$ с некоторым k. Естественно, что U будет снова перечислимо по Тьюрингу. Одновременно выполняются и требования 1)—3) определения 4.1:

$$1)\ U_m = \bigcup_{k=0}^{\infty} \{w \mid (k, m+k+1, w) \in T\} \supseteq$$
$$\supseteq \bigcup_{k=0}^{\infty} \{w \mid (k, m+1+k+1, w) \in T\} =$$
$$= U_{m+1} \qquad (m=0, 1, \ldots),$$

так как множество $\{(m, w) \mid (k, m, w) \in T\}$ для каждого k удовлетворяет требованию 1) определения 4.1;

2) U_m секвенциально как объединение секвенциальных множеств;

$$3)\ p(U_m) \leqslant \sum_{k=0}^{\infty} p(\{w \mid (k, m+k+1, w) \in T\}) \leqslant$$
$$\leqslant \sum_{k=0}^{\infty} \frac{1}{2^{m+k+1}} = \frac{1}{2^m}.$$

Произвольному фиксированному секвенциальному тесту K сопоставим теперь, как это было сделано выше, номер k. Тогда для $c=c_{UK}=k+1$

$$K_{m+c}=\{w \mid (k,\ m+c,\ w)\in T\}=\{w \mid (k,\ m+k+1,\ w)\in T\}\subseteq$$
$$\subseteq \sum_{k=0}^{\infty}\{w \mid (k,\ m+k+1,\ w)\in T\}=U_m.$$

Заметим, что U рекурсивио перечислимо. Все остальные утверждения теоремы непосредственно вытекают из определений.

Теперь мы попытаемся установить, чего же, собственно, мы добились этим определением понятия «случайной (бесконечной) 0-1-последовательности». До сих пор нас занимали лишь чисто внутренние определяющие черты нашей теории. Оказалось, однако, что практически все теоремы обычной теории вероятностей бесконечных 0-1-последовательностей (в предположении статистической незавнсимости компонент $x=x_1x_2\ldots$ и обращения их в 0 (как, впрочем, и в 1) с вероятностью $^1/_2$) являются источниками соответствующих секвенциальных тестов. Мы проиллюстрируем эту связь одним примером, который наверняка известен читателям, знакомым с теорией вероятностей.

Усиленный закон больших чисел в подходящей для нас формулировке утверждает, что в случайной 0-1-последовательности $x=x_1x_2\ldots$ должно встретиться приблизительно одииаковое число нулей и единиц, т. е. что

$$\lim_{n\to\infty}\frac{1}{n}(x_1+\ldots+x_n)=\frac{1}{2}.$$

В традиционной теории вероятностей известно следующее утверждение: для любого $\varepsilon>0$ открытые множества

$$U(\varepsilon,\ n)=\bigcup_{k\geqslant n}\left\{x \,\middle|\, \left|\frac{1}{k}(x_1+\ldots+x_k)\right|>\varepsilon\right\}$$

образуют в X убывающую последовательность, $\lim_{n\to\infty} p(U(\varepsilon,\ n))=0$, так что $N(\varepsilon)=\bigcap_n U(\varepsilon,\ n)$ есть нулевое миожество в смысле § 3. Мы можем, конечно, ограничиться для ε значениями $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots$. Таким образом, получаем бесконечную матрицу

$$\begin{matrix} U(1,\ 1), & U(1,\ 2), & U(1,\ 3), & \ldots \\ U\left(\frac{1}{2},\ 1\right), & U\left(\frac{1}{2},\ 2\right), & U\left(\frac{1}{2},\ 3\right), & \ldots \\ U\left(\frac{1}{3},\ 1\right), & U\left(\frac{1}{3},\ 2\right), & U\left(\frac{1}{3},\ 3\right), & \ldots \\ \cdots & \cdots & \cdots & \cdots \end{matrix}$$

и, ввиду того что $\lim\limits_{n\to\infty} p\left(U\left(\frac{1}{k},\ n\right)\right)=0$ $(k=1,\ 2,\ \ldots)$, нетрудно для каждого m выбрать такую последовательность $n_{m1},\ n_{m2},\ \ldots$, чтобы

$$p(U(1,\ n_{m1}))+p\left(U\left(\frac{1}{2},\ n_{m2}\right)\right)+\ldots\leqslant\frac{1}{2^m}.$$

Множество

$$U_m=U(1,\ n_{m1})\cup U\left(\frac{1}{2},\ n_{m2}\right)\cup\ldots$$

удовлетворяет, таким образом, требованию 3) определения 4.1:

$$p(U_m)\leqslant\frac{1}{2^m}.$$

Легко добиться дополнительно выполнения неравенств $n_{1k}\leqslant n_{2k}\leqslant\ldots$ $(k=1,\ 2,\ \ldots)$, из которых, очевидно, следует, что

$$U_1\supseteq U_2\supseteq\ldots.$$

Тем самым имеется все необходимое для определения секвенциального теста, исключая только вычислимость по Тьюрингу. Теперь можно выдвинуть следующие интуитивные доводы: легко установить перечислимость по Тьюрингу секвеициальных (§ 3) множеств слов $K\left(\frac{1}{k},\ n\right)$, для которых $\left[K\left(\frac{1}{k},\ n\right)\right]=U\left(\frac{1}{k},\ n\right)$. Представляется вполне убедительным, что теперь осталось найти лишь машинную процедуру вычисления n_{mk}. Для этого используют точные оценки значений $p\left(U\left(\frac{1}{k},\ n\right)\right)$, имеющиеся в готовом виде в обычной теории вероятностей; в остальном допустима полная свобода действий для выбора n_{mk}, лишь бы работа была доступна машине.

В заключение докажем еще один тесно связанный со всем предшествующим результат.

4.3. Теорема. *Случайные* 0-1-*последовательности не вычислимы по Тьюрингу.*

Доказательство. Пусть $x = x_1 x_2 \ldots$ есть некоторая вычислимая по Тьюрингу 0-1-последовательность. Определим секвенциальный тест K, положив $K_m = \{x_1 \ldots x_m y_{m+1} \ldots y_{m+s} \mid s \geqslant 0,\ y_{m+1}, \ldots, y_{m+s} = 0, 1\}$, так что $x \in M_K$[1]). Тем самым, согласно теореме 4.2, имеем также $x \in M$, т. е. x — не случайная последовательность.

Следующая теорема является в каком-то смысле обратной теореме 2.2:

4.4. Теорема. *Пусть* $f(n)$ $(n = 1, 2, \ldots)$ *есть вычислимая по Тьюрингу функция со значениями из множества* $\{0, 1, \ldots\}$, *для которой найдется вычислимая по Тьюрингу последовательность* $N_1 < N_2 < \ldots$ *натуральных чисел, такая, что*[2])

$$\text{(2)} \qquad \sum_{n=N_m}^{N_{m+1}-1} \frac{1}{2^{f(n)}} < \frac{1}{2^{m+1}} \qquad (m = 1, 2, \ldots).$$

Тогда любой случайной бесконечной 0-1-*последовательности* $x = x_1 x_2 \ldots$ *соответствует постоянная* $n(x)$, *такая, что для всех* $n \geqslant n(x)$

$$K(x_1 \ldots x_n) \geqslant n - f(n).$$

Доказательство. Используя полученную в теореме 1.2 асимптотически оптимальную рекурсивную функцию $A(* \mid *)$ и связанную с ней меру сложности $K(*)$, мы построим следующий секвенциальный тест K:

$K_0 = \Omega,$

$K_m = \{w = w_1 \ldots w_r \mid r \geqslant N_m,\quad K(w_1 \ldots w_r) < n - f(n)$ для подходящего n из отрезка $N_m \leqslant n \leqslant r\}$ $(m = 1, 2, \ldots)$.

---

[1]) $M_K = \{x\}$. — *Прим. перев.*

[2]) Пример функции $f(n)$: $f(n) = n^{\alpha}$, $0 < \alpha < 1$. — *Прим. перев.*

Итак, множество

$K_m = \{w = w_1 \ldots w_r \mid r \geqslant N_m$ и существуют n из отрезка $N_m \leqslant n \leqslant r$ и программа p длины $|p| < n - f(n)$, для которой $A(p \mid n) = w_1 \ldots w_n\}$

секвенциально, причем, очевидно, $K_0 \supseteq K_1 \supseteq \ldots$ и, наконец,

$$p(K_m) \leqslant \sum_{n=N_m}^{\infty} \frac{1}{2^n} \cdot (\text{число программ } p \text{ длины } |p| < n - f(n)) \leqslant$$

$$\leqslant \sum_{n=N_m}^{\infty} \frac{1}{2^n} 2^{n-f(n)} = \sum_{n=N_m}^{\infty} \frac{1}{2^{f(n)}} = \sum_{k=m}^{\infty} \sum_{n=N_k}^{N_{k+1}-1} \frac{1}{2^{f(n)}} <$$

$$< \sum_{k=m}^{\infty} \frac{1}{2^{k+1}} = \frac{1}{2^m}.$$

Таким образом, мы получили секвенциальный тест.

Согласно теореме 4.2, существует постоянная c, для которой $K_{m+c} \subseteq U_m$ $(m = 0, 1, \ldots)$. Пусть $x = x_1 x_2 \ldots$ случайна. Тогда имеется число m, для которого $x \notin [U_m]$, т. е. $x \notin [K_{m+c}]$, т. е. не существует $n \geqslant N_{m+c}$, удовлетворяющего неравенству $K(x_1 \ldots x_n) < n - f(n)$. Итак, $K(x_1 \ldots x_n) \geqslant n - f(n)$ для всех $n \geqslant N_{m+c}$.

ЛИТЕРАТУРА

1. Bernoulli J., Wahrscheinlichkeitsrechnung (Ars Conjectandi), Ostwalds Klassiker, Bd. 107, 108, Leipzig, 1899.
2. Blumenthal R. M., Getoor R. K., Markov Processes and Potential Theory, Academic Press, 1969.
3. Borel E., Méthodes et problèmes de la Théorie des Fonctions, 38—66, Paris, Gauthier-Villars, 1920.
4. Breiman L., Probability, Reading/Mass., Addison-Wesley, 1968.
5. Дынкин Е. Б., Марковские процессы, М., Физматгиз, 1963.
6. Hermes H., Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit, Berlin—Göttingen—Heidelberg, Springer, 1961.
7. Колмогоров А. Н., Основные понятия теории вероятностей, М.—Л., 1936.
8. Колмогоров А. Н., Три подхода к определению понятия информации, *Проблемы передачи информации*, 1 (1965), 3—11.
9. Martin-Löf P., Algorithmen und zufällige Folgen, Scriptum Erlangen, 1966.
10. Martin-Löf P., The definition of random sequences, *Information and Control*, 9 (1966), 602—619.

11. Mises R. V., Grundlagen der Wahrscheinlichkeitsrechnung, *Math. Z.*, 5 (1919), 52—99.
12. Mises R. V., Wahrscheinlichkeit, Statistik und Wahrheit, Wien, Springer, 1936.
13. Schnorr C. P., Eine Bemerkung zum Begriff der zufälligen Folge, *Z. Wahrscheinlichkeitstheorie* (1969).
14. Schnorr C. P., Über die Definition von effektiven Zufallstests, *Z. Wahrscheinlichkeitstheorie*, 15, № 4 (1970).
15. Ville J., Étude critique de la notion de collectif, Paris, Gauthier-Villars, 1939.
16. Wald A., Die Wiederspruchsfreiheit des Kollektivbegriffs der Wahrscheinlichkeitsrechnung, *Erg. math. Koll.*, 8 (1937), 38—72.
17. Wald A., Die Wiederspruchsfreiheit des Kollektivbegriffs, Colloque consacrè à la Théorie des Probabilités, Act. Sci. Ind. № 735, Paris, Hermann, 1938.
18*. Solomonoff R. J., A Formal Theory of Inductive Inference 1, *Information and Control*, 7, 1 (1964), 1—22.
19*. Колмогоров А. И., К логическим основам теории информации и теории вероятностей, *Проблемы передачи информации*, 3 (1969), 3—7.
20*. Church A., On the Concept of a Random Sequence, *Bull. Amer. Math. Soc.*, 46 (1940), 254—260.

МАШИННО-ПОРОЖДЕННЫЕ 0-1-ПОСЛЕДОВАТЕЛЬНОСТИ

К. ЯКОБС

Издавна проявления симметрии и упорядоченности побуждали математиков к важным и радующим своей красотой исследованиям. Те, кто изучал математику, знают о классификации групп кристаллографии, которая была осуществлена во второй половине XIX столетия Барковым, Федоровым, Жорданом, Шёнфлисом и Зонке, и, возможно, читали книгу Г. Вейля [10] или соответствующие разделы книг Кокстера [2] или Шпайзера [8] [1]).

Можно подыскивать разные психологические объяснения тому удовольствию, которое доставляют подобные исследования. Я полагаю, что в общем оно вызвано тем, что люди испытывают воодушевление, обнаруживая некоторую упорядоченность своего внутреннего мира. По-видимому, теория групп и исследования симметрии каким-то образом,— хотя бы на мгновения,— могут проецироваться во внутренний мир изучающих их людей. Изучение драгоценных минералов является дополнительным источником удовольствия при занятиях группами кристаллографии. Однако для настоящего математика главную ценность представляют красивые и тонкие соображения, на которые вдохновили его блестящие камни. Он будет склонен сделать еще один шаг и найдет особое удовольствие в продумывании теории, в которой материя вообще не играет никакой роли и только мысль сверкает своими духовными гранями.

Мне хотелось бы теперь попытаться — взяв за основу работы Хедлунда — Морса [3], Какутани [4] и Кини [5, 6] — дать читателю материал для таких размышлений. Фактура,

---

[1]) Или популярную книгу Гильберта и Кон-Фоссена [11].— *Прим. перев.*

используемая для построения рассматриваемых объектов, скудна и невзрачна — символы 0 и 1. Из них мы строим не только конечные блоки, например такие:

0, 01, 001, 110, 0110, 1001, ... ,

но также и бесконечные последовательности, например такие:

000 ... ,
0101 ... ,
001001 ... ,
0110|1001|1001|0110| ... ,
001|001|110|001|001|110|110|001| ...

и, вообще,

$$\omega = \omega_0\omega_1\omega_2 \ \dots,$$

где $\omega_t = 0$ или 1 ($t = 0, 1, \dots$). Мы будем избегать разделения символов запятой и лишь изредка при необходимости будем пользоваться вертикальным штрихом для облегчения зрительного восприятия. Так как все блоки и все последовательности состоят из нулей и единиц, то мы будем говорить о 0-1-*блоках* и 0-1-*последовательностях*.

Читатель уже, наверное, усмотрел в приведенных выше последовательностях некую симметрию, присутствие которой позволяет, например, автоматически продолжать их на бумажной ленте с помощью простых машин до бесконечности.

Цель этой статьи состоит в уточнении свойств симметрии последовательностей, каждая из которых может быть получена посредством некоторой определенной процедуры, реализуемой с помощью *машин* и *программ*. Так как речь идет о бесконечных последовательностях, то в отличие от групп кристаллографии мы приходим к необходимости иметь дело с *бесконечными симметриями*. Одна из главных задач состоит в том, чтобы выработать приемы изучения бесконечных симметрий, использующие конечные построения.

Схема работы интересующих нас машин допускает математическую формализацию с помощью некоторой *алгебры блоков*, обязанной своим возникновением *Кини* [6]. Мы расскажем о ней в § 1 и покажем, как она может быть реализована с помощью машины. Все дальнейшее излагается на языке алгебры блоков, но мы хотим посоветовать читателю постоянно представлять себе работающую машину. Затем в § 2 мы покажем, что порождаемые таким образом последовательности будут, вообще говоря, не периодическими, и докажем теорему 2.4, имеющую нечто общее с *правилом троекратного повторения позиции в шахматах.*

В § 3 мы вводим понятие *почти-периодичности* и показываем, что все наши последовательности почти-периодичны. В § 4 будут рассмотрены задачи о средних значениях, например вопросы об *относительной частоте* нулей и единиц в наших последовательностях. В § 5 будет показано, что в наших, как правило, непериодических последовательностях имеется на самом деле *бесконечнократная периодичность*, если только дать ей правильное, т. е. точно обоснованное, истолкование. В § 6 перечислены задачи, на которых читатель сможет себя проверить как для того, чтобы ближе познакомиться с изложенным материалом, так и для того, чтобы воспринять его как фрагмент некоторой более общей, отчасти еще не завершенной теории.

Развиваемая здесь вполне элементарными средствами теория имеет приложения в топологической динамике и эргодической теории, для чего следует обратиться к топологическим и метрическим методам. Пространство всех 0-1-последовательностей является на самом деле известным метрическим компактом, в котором теория меры уже давно была развита математиками, работающими в эргодической теории и теории вероятностей [1]). Именно отсюда ведет свое происхождение большая часть представленных здесь результатов. Некоторые из рассмотренных нами исследований были проведены впервые только в 1966 г. Но их предыстория восходит к сравнительно давнему времени (ср. Морс [7], Туэ [9]).

---

[1]) Описание этого компакта дано в статье «Машины Тьюринга и случайные 0-1-последовательности» этой книги.—*Прим. перев.*

§ 1. Один алгоритм порождения 0-1-последовательностей

В этом параграфе мы опишем один метод порождения 0-1-последовательностей, который будет сформулирован нами в виде алгоритма, допускающего простую машинную реализацию.

1. Подготовительное упражнение со специальными последовательностями

Если вы не спешите, читатель, попробуйте самостоятельно установить, согласно каким правилам должны быть продолжены до бесконечности последовательности

0000 ... ,
01010101 ... ,
001001001 ... ,
0110|0110 ... ,
0110|1001|1001|0110| ... ,
001|001|110|001|001|110|110|110|001| ... .

Вертикальные штрихи по-прежнему служат лишь для зрительной ориентировки. Только две последние последовательности нетривиальны; предпоследняя придумана М. Морсом и называется *последовательностью Морса*. Последняя была указана М. Кини и будет здесь поэтому называться (тернарной) *последовательностью Кини*; тот кто слышит «внутреннюю музыку» этой последовательности, мог бы назвать ее «вальсом бесконечного порядка».

2. Алгебра блоков

Конечная упорядоченная серия $A=a_0 \ldots a_{m-1}$ нулей и единиц будет называться *0-1-блоком A длины* $|A|=m$. При этом $a_0, \ldots, a_{m-1}$ называются 0-й, ..., $(m-1)$-й *компонентами* (буквами, символами, ...) блока; в предыдущих примерах нам встречались среди прочих блоки 0, 01, 001, 0110, 1001.

Мы введем теперь два вида соединения блоков и познакомимся с правилами, согласно которым можно производить вычисления над этими соединениями. Порожденную этими соединениями совокупность операций над блоками (Кини [6]) мы можем рассматривать как некоторую примитивную *алгебру блоков*.

Первое соединение состоит просто в *последовательном выписывании компонент обоих блоков*. Пусть $A=a_0\dots$ $\dots a_{m-1}$, $B=b_0 \dots b_{n-1}$ суть два 0-1-блока; положим

$$AB=a_0 \dots a_{m-1}b_0 \dots b_{n-1}.$$

Длины блоков при этом складываются:

$$|AB|=|A|+|B|.$$

Мы назовем эту операцию *сложением* блоков. Естественно, что оно не коммутативно, но ассоциативно, поэтому мы можем выписывать в ряд одну за другой произвольно длинные и даже бесконечные серии блоков с произвольной расстановкой скобок или даже вовсе без скобок; в последнем случае возникает бесконечная 0-1-последовательность. Можно было бы выбрать в качестве нейтрального элемента при сложении «пустой блок» длины 0, но это нам не понадобится.

Второе соединение использует сложенне и еще одну операцию, которую можно назвать *отражением* и которая действует на символы 0,1 согласно равенствам

$$0^0=0,\ 0^1=1,\ 1^0=1,\ 1^1=0,$$

а на блок A действует покомпонентно согласно равенствам

$$A^0=A,\ A^1=a_0^1 \dots a_{m-1}^1 \qquad (A=a_0\dots a_{m-1}).$$

Таким образом, собственно отражение символически изображается показателем 1. (При случае мы будем подвергать отражению и 0-1-последовательности: если $\omega=\omega_0\omega_1\dots$, то $\omega^1=\omega_0^1\omega_1^1\dots$.) Имеем, например,

$$(01)^1=10,\quad (0110)^1=1001,\quad (001)^1=110.$$

Мы введем теперь операцию *умножения* 0-1-блоков. Если $A=a_0\dots a_{m-1}$, $B=b_0\dots b_{n-1}$ суть 0-1-блоки, то мы положим

$$A\times B=A^{b_0}\dots A^{b_{n-1}}$$

и назовем этот блок произведением A и B. Длины блоков при этом перемножаются:

$$|A\times B|=|A|\cdot|B|.$$

Объединив в отдельный блок компоненты произведения $A\times B$ с номерами $\equiv k(\mathrm{mod}\,|A|)$ с сохранением их порядка, мы получим в точности блок $B^{a_k}(k=0, \ldots, n-1)$.

Блок 0 при умножении ведет себя как левая и правая единица, умножение на 1 слева или справа действует как отражение. Как видно из примера

$$(01)\times(00)=0101\neq 0011=(00)\times(01),$$

блоки длины 2, вообще говоря, не коммутируют, хотя

$$0\times 1=1\times 0\,(=1)\ \text{ и }\ (01)\times(10)=1001=(10)\times(01).$$

Вот еще несколько примеров произведений блоков:

$$(01)\times(01)=0110,\ (0110)\times(01)=01101001,$$
$$(001)\times(001)=001001110.$$

Правила вычислений

$$(1)\qquad A\times(BC)=(A\times B)(A\times C),$$
$$(2)\qquad (A\times B)^1=A^1\times B=A\times B^1$$

очевидны.

Умножение 0-1-блоков ассоциативно:

$$(3)\qquad (A\times B)\times C=A\times(B\times C);$$

действительно, при $|C|=1$ имеем

$$(A\times B)\times 0=A\times B=A\times(B\times 0),$$
$$(A\times B)\times 1=(A\times B)^1=A\times B^1=A\times(B\times 1).$$

Допустим, что (3) выполняется для C; тогда, используя (1), получаем

$$(A\times B)\times(C0)=[(A\times B)\times C]\,[A\times B]=[A\times(B\times C)][A\times B]=$$
$$=A\times[(B\times C)\,B]=A\times[B\times(C0)].$$

Точно так же ввиду (1) и (2) имеем

$$(A\times B)\times(C1)=[(A\times B)\times C][A\times B]^1=[A\times(B\times C)][A\times B^1]=$$
$$=A\times[(B\times C)\,B^1]=A\times[B\times(C1)],$$

и доказательство соотношения (3) получается индукцией по $|C|$.

Ассоциативность позволяет нам писать произвольно длинные произведения блоков с произвольной расстановкой скобок или вовсе без скобок. При определенных условиях имеют смысл даже *бесконечные* произведения блоков. В самом деле, очевидно, что $A \times B$ начинается с блока A тогда и только тогда, когда B начинается с 0. Итак, если $P_1, P_2, \ldots$ суть произвольные блоки, то частные произведения

$$A \times (0P_1) \times \ldots \times (0P_n)$$

бесконечного произведения

$$A \times (0P_1) \times (0P_2) \times \ldots \tag{4}$$

являются последовательными продолжениями одно другого и образуют тем самым определенные отрезки (длины $|A| \cdot |0P_1| \cdot \ldots \cdot |0P_n|$) некоторой бесконечной 0-1-последовательности $\omega = \omega_0 \omega_1 \ldots$, которую мы и будем рассматривать как значение бесконечного произведения (4):

$$\omega = \omega_0 \omega_1 \ldots = A \times (0P_1) \times (0P_2) \times \ldots .$$

Объектом наших дальнейших исследований и будут как раз последовательности, получаемые в виде бесконечных произведений из некоторого *начального блока* A и начинающихся с 0 блоков $0P_1$, $0P_2$, $\ldots$. Имеем, например:

$$\begin{aligned}
000\ldots &= 0 \times (00) \times (00) \times \ldots ,\\
0101\ldots &= (01) \times (00) \times (000) \times \ldots = \\
&= (010) \times (010) \times \ldots ,\\
01101001\ldots &= 0 \times (01) \times (01) \times (01) \times \ldots ,\\
001001110\ldots &= 0 \times (001) \times (001) \times (001) \times \ldots .
\end{aligned}$$

Последовательности Морса и Кини также могут быть представлены в виде бесконечных произведений. Так как произведения допускают, кроме того, произвольные подразделения, то такое представление не является, конечно, однозначным; можно, например, записать последовательность Морса как в виде

$$(0110) \times (0110) \times \ldots ,$$

так и в виде

$$(01) \times (0110) \times (01101001) \times \ldots .$$

При этом становится очевидной скрытая симметрия последовательности Морса, что побуждает нас продумать соответствующие возможности и для тернарной последовательности Кини.

Последовательность Морса является лишь примером из класса всех произведений следующего специального вида:

$$(5)\qquad 0\times(0p_1)\times(0p_2)\times\ldots\ ,$$

где p_k принимает значение 1 для бесконечного числа k и значение 0 — для остальных k. Рассматривая произведения

$$\underbrace{(00)\times(00)\times\ldots\times(00)}_{q\ \text{пар}}\times(01)=\underbrace{00\ldots00}_{2^q\ \text{нулей}}\underbrace{11\ldots11}_{2^q\ \text{единиц}},$$

мы убеждаемся в том, что 0-1-последовательности (5) могут быть также представлены в виде

$$(5a)\qquad 0\times(0P_1)\times(0P_2)\times\ldots,$$

где

$$(5b)\qquad 0P_n=\underbrace{0\ldots0}_{2^{q_n}}\underbrace{1\ldots1}_{2^{q_n}}\quad (\text{для подходящих } q_1,\ q_2,\ \ldots).$$

Так как этот класс последовательностей был рассмотрен первоначально Какутани [4], то мы и будем называть их *последовательностями Какутани*. Последовательность Морса получается из последовательности Какутани при $q_1=q_2=\ldots=0$. Непосредственно видно, что разные последовательности $q_1,\ q_2,\ \ldots$ порождают разные последовательности Какутани. Первое несовпадение q_k для двух последовательностей уже приводит к различию. Таким образом, имеется *континуум* последовательностей Какутани.

В некоторых случаях целесообразно рассматривать *произведение блока B и бесконечной последовательности* $\eta=\eta_0\eta_1\ldots$; оно определяется как бесконечная последовательность

$$B\times\eta=B^{\eta_0}B^{\eta_1}\ldots\ ,$$

получаемая из 2 заменой каждого символа 0 блоком B, а каждого символа 1 — блоком B^1.

Каждая 0-1-последовательность, которая может быть образована последовательным покомпонентным выписыванием блоков A и A^1, допускает такое представление. В частности, для последовательности $\omega = A\times(0P_1)\times\times(0P_2)\times\dots$ и произвольного $n>0$ можно получить представление

$$\omega = B_n \times \eta_n,$$

где $B_n = A\times(0P_1)\times\dots\times(0P_n)$, $\eta_n = (0P_{n+1})\times\dots$. Из (2) вытекает тогда, кроме того, что

$$\omega^1 = B_n^1 \times \eta_n = B_n \times \eta_n^1,$$

где введение верхнего индекса 1 означает также и в случае бесконечных последовательностей отражение, т. е. замену 0 на 1 и 1 на 0.

В качестве примера можно записать последовательность Морса для любого $n>0$ в виде

$$01101001\ldots = (\underbrace{(01)\times\dots\times(01)}_{n})\times(01101001\ldots)$$

и аналогично тернарную последовательность Кини в форме

$$001001110\ldots = (\underbrace{(001)\times\dots\times(001)}_{n})\times(001001110\ldots).$$

Подумайте, какой наглядный смысл заключен в этой записи.

3. Машинное представление

Бесконечное произведение

$$A\times(0P_1)\times(0P_2)\times\dots$$

может быть следующим образом порождено некоторой машиной, которая в рабочие циклы № 1, 2, ... заполняет нулями и единицами ячейки бесконечной в одну сторону бумажной ленты.

Перед выполнением первого рабочего цикла начальный блок уже выписан в самом начале бумажной ленты, все остальные ячейки которой пусты. За первый рабочий цикл машина печатает в соответствии с *программным блоком* $P_1 = p_1\dots p_{r_1}$ и непосредственно после уже напечатанного блока A блоки $A^{p_1}, \dots, A^{p_{r_1}}$ в указанной последовательности. Итогом работы первого рабочего цикла является запись блока $A\times(0P_1)$ в самом начале ленты, остальные ячейки которой пусты.

В такой исходной ситуации машина приступает к выполнению второго рабочего цикла и делает то же, но теперь с программным блоком P_2 и блоком $A\times(0P_1)$ вместо прежнего начального блока A.

Ясно, что происходит дальше. Машина должна при этом, очевидно, только читать произвольно длинные блоки, запоминать их, а затем в соответствии с конечным программным блоком снова печатать в том же или «отраженном» виде. Используя пометки, которые машина временно наносит на ленту в процессе работы, можно опять устранить требование неограниченно большой памяти[1]).

4. Пространство сдвигов

Чтобы иметь более удобные обозначения, целесообразно интерпретировать 0-1-последовательности как точки в так называемом *пространстве Бернулли*, или *пространстве сдвигов*,

$$\Omega=\{\omega=\omega_0\omega_1\ldots|\omega_t=0 \text{ или } 1\ (t=0, 1, \ldots)\}.$$

Для каждого 0-1-блока $A=a_0\ldots a_{m-1}$ мы образуем *соответствующий A (специальный) цилиндр* в Ω, являющийся подмножеством Ω:

$$[A]=[a_0\ldots a_{m-1}]=\{\omega=\omega_0\omega_1\ldots|\,\omega_0=a_0, \ldots, \omega_{m-1}=a_{m-1}\}.$$

Характеристическую функцию произвольного подмножества $F\subset\Omega$ мы будем коротко обозначать 1_F:

$$1_F(\omega)=\begin{cases}1, & \text{если } \omega\in F,\\ 0, & \text{если } \omega\notin F.\end{cases}$$

Вместо $1_{[A]}$ будем писать просто 1_A.

---

[1]) Эта довольно искусственная и малосодержательная конструкция не является вычислительной процедурой в смысле Тьюринга, хотя описанная здесь машина является, конечно, машиной Тьюринга (см., например, требования 1.2 и 1.8 п. 4 § 1 первой статьи этой книги).— *Прим. перев.*

Наконец, при помощи соотношения

$$T:\omega=\omega_0\omega_1\ldots\to\omega T=\omega_1\omega_2\ldots$$

мы определим отображение Ω на себя, которое мы будем называть *сдвигом*. Мы пишем знак отображения справа от объекта, на который оно действует;

$$1_A(\omega T^t)=1,\text{ т. е. }\omega T^t\in A,$$

означает, таким образом, что

$$\omega_t=a_0,\ \ldots,\ \omega_{t+m-1}=a_{m-1},$$

а это последнее означает, что *блок* A *входит в* ω *с* t*-й позиции*.

Мы распространим эту терминологию также и на *вхождения блоков в другие блоки*, причем нумерацию позиций будем вести с 0. Например, вхождение A в A^1A в качестве правой половины этого блока выражают так: A входит в A^1A с $|A|$-й позиции. Разумеется, блок длины r может входить в блок длины n только с позиции $\leqslant n-r$.

§ 2. Апериодичность

Мы хотим показать, что последовательности

$$\omega=A\times(0P_1)\times(0P_2)\times\ldots$$

периодичны только в очень специальных случаях. Сначала рассмотрим два примера.

2.1. Пример. Существует n, для которого

$$(1)\qquad \eta=(0P_{n+1})\times(0P_{n+2})\times\ldots=00\ldots;$$

положив

$$C_n=A\times(0P_1)\times\ldots\times(0P_n),$$

получим

$$\omega=C_n\times\eta=C_nC_n\ldots,$$

и ω периодично с периодом $|C_n|$—длиной C_n. Условие (1) эквивалентно требованию $0P_k=00\ldots0$ $(k>n)$.

2.2. Пример. Существует $n>0$, для которого

$$0P_k=010\ldots10\qquad(k>n),$$

так что

$$\eta = (0P_{n+1}) \times (0P_{n+2}) \times \ldots = 010101\ldots;$$

обозначив $C_n = A \times (0P_1) \times \ldots \times (0P_n)$, получим

$$\omega = C_n C_n^1 C_n C_n^1 \ldots,$$

так что периодом является число $2 \cdot |C_n|$.

Мы покажем теперь, что этими примерами исчерпываются периодические случаи.

2.3. Теорема. *Если последовательность*

$$\omega = A \times (0P_1) \times (0P_2) \times \ldots$$

периодична, то имеет место один из следующих двух случаев:

1) *существует* $n_0 > 0$, *для которого*

$$0P_k = 010\ldots10 \qquad (k > n_0);$$

2) *существует* $n_0 > 0$, *для которого*

$$0P_k = 00\ldots0 \qquad (k > n_0).$$

Доказательство. Заменив в случае необходимости A на A^1, т. е. произведя покомпонентное отражение ω, мы можем считать, что ω начинается с 0. Пусть s есть наименьший положительный период ω и $B = b_0 \ldots b_{s-1} = \omega_0 \ldots \omega_{s-1}$, так что

$$\omega = BB\ldots .$$

Для каждого n положим

$$C_n = A \times (0P_1) \times \ldots \times (0P_n).$$

Случай I. Существует n, для которого $|B|$ делит $|C_n|$. Тогда C_n имеет вид $C_n = BB\ldots B$, и для последовательности $(0P_{n+1}) \times (0P_{n+2}) \times \ldots$, согласно которой происходит формирование $\omega = BB\ldots$ из блоков C_n и C_n^1, остается единственная возможность

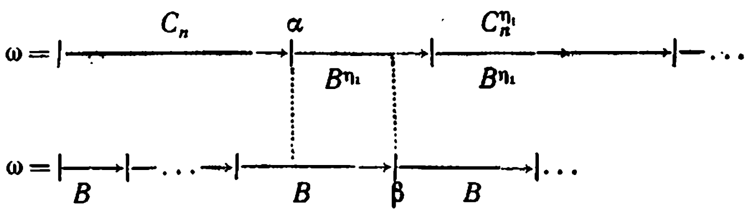
$$(0P_{n+1}) \times (0P_{n+2}) \times \ldots = 000\ldots,$$

откуда и следуют равенства $0P_k = 00\ldots0$ $(k > n)$, а вместе с ними и первая часть нашей теоремы.

Случай II. Не существует n, для которого $|B|$ делит $|C_n|$. Написав $(0P_{n+1})\times(0P_{n+2})\times\ldots=\eta=\eta_0\eta_1\eta_2\ldots=$ $=0\eta_1\eta_2\ldots$, мы получим для ω два представления

$$\omega=C_nC_n^{\eta_1}\ldots,$$
$$\omega=BBB\ldots,$$

причем место соединения блоков C_n и $C_n^{\eta_1}$ перекрывается блоком B; если n настолько велико, что $|C_n|>2|B|$, то возникшая ситуация может быть схематически представлена так:



Заметим, что сам блок $C_n^{\eta_1}$ начинается с блока $B^{\eta_1\eta_1}$. Мы рассмотрим два подслучая.

Подслучай А. $\eta_1=0$. Из рисунка видно, что последовательность $\omega=BB\ldots$ может быть переведена в $BB\ldots$, т. е. в себя, сдвигом на число, меньшее $|B|$[1]), что противоречит минимальности периода $|B|$.

---

[1]) Точнее, из рисунка видно, что место соединения α блоков C_n и $C_n^{\eta_1}$ разбивает перекрывающий его блок B на сумму $B=B_1B_2$, где $0<|B_1|$, $|B_2|<|B|$, а место соединения β соответствующих блоков B_1 и B_2 разбивает начальный блок B^{η_1} блока $C_n^{\eta_1}$ на сумму $B^{\eta_1}=B_2B_1$.

Из равенств

$$(*)\qquad B^{\eta_1}=B_1^{\eta_1}B_2^{\eta_2}=B_2B_1$$

при $\eta_1=0$ следует, что

$$B=B_1B_2=B_2B_1$$

и

$$\omega=BB\ldots=B_1B_2B_1B_2\ldots=B_2B_1B_2B_1\ldots,$$

откуда $\omega T^{|B_1|}=\omega T^{|B_2|}=\omega$.— *Прим. перев.*

Подслучай B. $\eta_1=1$. Из рисунка видно, что последовательность $\omega=BB\ldots$ может быть переведена в $B^1B^1\ldots=\omega^1$ сдвигом на некоторое $r<|B|$, а сдвигом на $2r<2|B|$ — в себя [1]). Из минимальности периода $|B|$ мы сразу получаем равенство $r=|B|/2$ и тем самым

$$C_nC_n^1=BB\ldots B,$$

откуда

$$\omega=C_nC_n^1C_nC_n^1\ldots,$$

т. е.

$$\eta=0101\ldots .$$

Это возможно только при $0P_k=0101\ldots10$ $(k>n)$, что и было описано во второй части нашей теоремы.

Замечание. Из теоремы 2.3 следует, что почти все последовательности Какутани непериодичны. Среди них имеется континуум непериодических [2]).

Из теоремы 2.3 мы заключаем, например, что последовательность Морса и тернарная последовательность Киии апериодичны. Последовательность Морса обладает даже еще более сильным свойством апериодичности.

2.4. Теорема (Хедлунд—Морс [3]). *Если $D=d_0\ldots d_{r-1}$ — произвольный 0-1-блок, то блок $DDd_0=$ $=d_0\ldots d_{r-1}d_0\ldots d_{r-1}d_0$ не имеет вхождений в последовательность Морса*

$$\omega=01101001\ldots=(01)\times(01)\times(01)\times\ldots .$$

Замечание. В последовательности Морса бесконечно часто встречаются изолированные вхождения DD для

---

1) Согласно предыдущему примечанию, из равенства (*) при $\eta_1=1$ получаем

$$B=B_1^1B_2^1=B_2B_1,$$

откуда

$$\omega=BB\ldots=B_1^1B_2^1B_1^1B_2^1\ldots=B_2B_1B_2B_1\ldots$$

и

$$\omega T^{|B_1|}=\omega T^{|B_2|}=\omega^1. \text{— } \textit{Прим. перев.}$$

2) Периодические последовательности Какутани ω, очевидно, удовлетворяют условию $p_k=0$ для всех $k>n_0(\omega)$, и их множество счетно.— *Прим. перев.*

произвольно длинных блоков D: можно, например, положить $D=(01)\times\ldots\times(01)$ (с произвольным числом сомножителей), так что

$$\omega=D\times(01)\times(01)\times\ldots=D\times\omega=DD^1D^1DD^1DDD^1\ldots.$$

Однако, согласно сформулированной теореме, всякая возможность дальнейшего повторения исключена.

Согласно известному *правилу троекратного повторения позиции в шахматах* партия прекращается (с ничейным результатом), если последовательность ходов, начнная с некоторого хода, целиком повторилась, а затем снова был повторен этот ход (это не соответствует международным правилам, глубже вникающим в структуру шахматной игры, ср., например, [1][1])). Если перевести это правило на язык 0-1-последовательностей, то можно сказать, что применение этого правила никогда не оборвет процесс посимвольной записи последовательности Морса.

Доказательство теоремы 2.4. Сначала мы покажем, что блок DDd_0 не входит в ω, когда длина r блока D есть *нечетное* число. Для $r=1$ это очевидно: здесь $DDd_0=d_0d_0d_0=000$ или 111; но ни один из этих блоков не входит в ω, так как каждый входящий в ω блок длины 3 содержит некоторый блок длины 2, входящий в ω с четной позиции, т. е. блок 01 или 10.

Если $r>1$, то $r\geqslant 3$ и $|DDd_0|\geqslant 7$. Заметим теперь, что, согласно представленню $\omega=(0110)\times(01101001\ldots)$, последовательность ω составлена из блоков 0110, 1001, которые, следовательно, входят в ω, начиная с позиций, кратных четырем ($4k$, $k=0, 1, \ldots$). Каждый входящий в ω блок длины 7 целиком включает в себя хотя бы один из этих блоков 0110, 1001. Итак, если блок DDd_0 входит в ω, то он содержит один из блоков 00 или 11. Мы разберем только случай, когда этот блок есть 00; для блока 11 все проходит точно так же. В блоке DDd_0 блок 00 может находиться в левом D, в правом Dd_0 либо на границе между ними. Так как, однако, блок Dd_0 начинается с d_0, то в любом случае 00 входит в правый Dd_0, и при этом он также встречается в DDd_0 слева от этого вхождения на расстоянии $|D|$. Итак, 00 входит

[1]) Или [12] — *Прим. перев.*

в ω в двух позициях, разность номеров которых есть нечетное число:

$$\begin{array}{ccccc} d_0 & & d_0 & & d_0 \\ | & \longrightarrow & | & \longrightarrow & | \\ & 00 & & 00 & \end{array}$$

Номер одной из этих позиций есть четное число. Но ввиду $\omega=(01)\times(01101001\ldots)$ на четных местах могут быть лишь блоки 01 или 10, в чем и состоит противоречие.

Пусть теперь $r=|D|>1$ есть *четное* число. Предположим, что $DDd_0=d_0\ldots d_{r-1}d_0\ldots d_{r-1}d_0\ldots$ входит в ω с t-й позиции.

Случай I: *t нечетно*. Тогда $t>0$ и $t-1$ четно. В позиции $t-1$ находится 01 или 10. Из соображений симметрии достаточно рассмотреть 01. Тогда имеем $d_0=1$. Число $t+r-1=(t-1)+r$ четно как сумма двух четных чисел. В этой позиции опять стоит 01 или 10, но, с другой стороны, $d_{r-1}d_0$, где $d_0=1$. Таким образом, $d_{r-1}=0$ и на $(t+r-1)$-й позиции находится 01.

Аналогично проверяется, что в $(t+2r-1)$-й позиции (опять четной!) снова стоит 01. Итак, блок

$$DDd_0=1d_1\ldots 01d_1\ldots 01$$

входит в ω непосредственно вслед за 0; блок

$$0DDd_0=01d_1\ldots 01d_1\ldots 01$$

находится в ω на *четной* позиции $t-1$. Следовательно, этот блок составлен из $2\frac{r}{2}+1$ блоков 01 и 10, и он может быть также записан в виде

$$0DDd_0=E_0\ldots E_{r/2}E_0\ldots E_{r/2}E_0,$$

где $E_0=01$ и $E_j=01$ или 10.

Используя представление $\omega=(01)\times(01101001\ldots)$, так сказать, в обратном направлении, получаем: в ω входит блок $D_0D_0e_0=e_0\ldots e_{r/2}e_0\ldots e_{r/2}e_0$ [1]), где

$$e_j=\begin{cases} 0, & \text{если } E_j=01, \\ 1, & \text{если } E_j=10. \end{cases}$$

Таким образом, $|D_0|=\frac{r}{2}+1$.

---

[1]) Согласно представлению $\omega=(01)\times\omega$,

$0DDd_0=(01)\times(D_0D_0e_0)$.— *Прим. перев.*

Случай II: t *четно*. Тогда $d_0d_1=01$ или 10. Из соображений симметрии достаточно рассмотреть только случай $d_0d_1=01$. Как и в случае I, получаем

$$DDd_0=01\ldots d_{r-1}01\ldots d_{r-1}0.$$

С четной позиции $t+2r$ начинается 01 или 10. Так как там находится последний элемент 0 блока DDd_0, то речь может идти только о блоке 01. Итак, ω содержит блок

$$DDd_01=01\ldots d_{n-1}01\ldots d_{n-1}01,$$

начинающийся в ω с четной позиции t; тем самым, как следует из рассуждения, аналогичного вышеприведенному, ω содержит также и блок $D_0D_0e_0=e_0\ldots e_{r/2}e_0\ldots e_{r/2}e_0$, где $e_0=0$. И снова $|D_0|=\frac{r}{2}+1$.

Таким образом, в обоих случаях возможна редукция от r к $\frac{r}{2}+1$. Если при повторном применении этого процесса мы придем к нечетному r, то возникает уже рассмотренная ситуация, и доказательство закончено. Если же мы будем последовательно уменьшать r вплоть до значения $r=4$ и не встретим нечетных r, то следующий шаг приведет нас к $r=3$, т. е. к уже разобранному случаю.

Тем самым все доказано.

§ 3. *Почти-периодичность*

Хотя 0-1-последовательности вида

$$\omega=A\times(0P_1)\times\ldots \tag{1}$$

периодичны только в исключительных точно описываемых случаях, все они обладают одним свойством, которое на первый взгляд является лишь ненамного более общим.

3.1. Определение. 1) Множество $M\subseteq Z^+=\{0,\ 1,\ldots\}$ называется *плотным*, если существует целое $L>0$, такое, что среди любых L следующих непосредственно друг за другом целых чисел из Z^+ найдется хотя бы одно принадлежащее M:

$$M\cap\{s,\ s+1,\ \ldots,\ s+L-1\}\neq\varnothing \qquad (s=0,\ 1,\ \ldots).$$

2) 0-1-последовательность $\omega=\omega_0\omega_1\ldots\in\Omega$ называется *почти-периодической*, если каждый входящий в ω блок является плотно входящим: если B есть 0-1-блок, то множество

$$\{t \mid t\geqslant 0,\ 1_B(\omega T^t)=1\}\subseteq Z^+$$

плотно или пусто.

Периодическая последовательность является, разумеется, почти-периодической. Более того, имеет место

3.2. Теорема. *Каждая последовательность вида*

$$\omega=A\times(0P_1)\times\ldots$$

почти-периодична.

Доказательство. Если она не периодична, то каждому $n>0$ соответствует $j>0$ (ср. примеры 2.1 и 2.2), такое, что в блоке

$$(0P_{n+1})\times\ldots\times(0P_{n+j})$$

встречается по крайней мере один символ 1 (помимо по крайней мере одного 0). Если обозначить

$$A\times(0P_1)\times\ldots\times(0P_r)=C_r\qquad(r=1,\ 2,\ \ldots),$$

то в C_{n+j} войдет как C_n, так и C_n^1, и то же будет верно, разумеется, и для C_{n+j}^1. Но ω получается соединением блоков C_{n+j} и C_{n+j}^1. Тем самым для $L=2|C_{n+j}|$ каждый блок $\omega_s\omega_{s+1}\ldots\omega_{s+L-1}$ содержит C_n.

Пусть теперь B — произвольный 0-1-блок, входящий в ω. Тогда для подходящего n он входит уже в C_n. Приведенное выше рассуждение показывает, что

$$\{t \mid 1_B(\omega T^t)=1\}\cap\{s,\ s+1,\ \ldots,\ s+L-1\}\neq\varnothing$$
$$(s=0,\ 1,\ \ldots),$$

и тем самым все доказано.

Континуум непериодических последовательностей вида (1), существующих согласно теореме 2.3, доставляет нам примеры непериодических почти-периодических последовательностей.

§ 4. Средние значения

Мы займемся теперь *относительной частотой* вхождения блоков в наши бесконечные последовательности-произведения. Здесь особенно хорошо видна целесообразность обозначений для сдвигов и *характеристических функций:* последние можно рассматривать как числа.

1. Общие соображения

4.1. Определение. Пусть

$$\omega = \omega_0\omega_1 \ldots$$

есть произвольная 0-1-последовательность и B — произвольный 0-1-блок.

1) Число
$$\frac{1}{t}\sum_{u=0}^{t-1} 1_B(\omega T^{s+u})$$

называется *относительной частотой* вхождения блока B в ω на отрезке от s до $s+t-1$.

2) Говорят, что блок B является *чезаровским* для ω, если существует предел

$$\bar{1}_B(\omega) := \lim_{t\to\infty} \frac{1}{t}\sum_{u=0}^{t-1} 1_B(\omega T^u).$$

Число $\bar{1}_B(\omega)$ называют в этом случае *средней частотой* вхождения B в ω.

3) Говорят, что блок B является *равномерно чезаровским* для ω, если

$$\bar{1}_B(\omega) = \lim_{t\to\infty} \frac{1}{t}\sum_{u=0}^{t-1} 1_B(\omega T^{s+u})$$

равномерно по $s=0, 1, \ldots$.

4) Говорят, что ω — *чезаровская последовательность*, если каждый блок в ω является чезаровским для ω; ω — *равномерно чезаровская последовательность*, если каждый блок в ω является равномерно чезаровским для ω.

Периодические последовательности тривиальным образом являются равномерно чезаровскими.

Простой результат о почти-периодических последовательностях содержит

4.2. Теорема. *Если* $\omega=\omega_0\omega_1\dots$ *почти-периодична и блок* B *входит в* ω, то

$$\varliminf_{t\to\infty}\left[\inf_{s\geqslant 0}\frac{1}{t}\sum_{u=0}^{t-1}1_B(\omega T^{s+u})\right]>0.$$

Если, в частности, B *является чезаровским для* ω, *то*

$$\bar{1}_B(\omega)>0.$$

Доказательство. Существует такое $L>0$, что для каждого $s\geqslant 0$ по крайней мере одно из L чисел

$$1_B(\omega T^s),\ \dots,\ 1_B(\omega T^{s+L-1})$$

равно 1. Отсюда следует, что

$$\inf_{s\geqslant 0}\frac{1}{L}\sum_{u=0}^{L-1}1_B(\omega T^{s+u})\geqslant\frac{1}{L}.$$

Если теперь $t>L$, то мы разобьем последовательность

$$1_B(\omega T^s),\ \dots,\ 1_B(\omega T^{s+t-1})$$

на k отрезков длины L и остаток длины $r<L$. Таким образом, $t=kL+r$ и

$$\frac{1}{t}\sum_{u=0}^{t-1}1_B(\omega T^{s+u})\geqslant\frac{kL}{kL+r}\cdot\frac{1}{L}-\frac{r}{t}.$$

При $t\longrightarrow\infty$ имеем также $k\longrightarrow\infty$, в то время как r остается ограниченным. Отсюда следует, что

$$\varliminf_{t\to\infty}\left[\inf_{s\geqslant 0}\frac{1}{t}\sum_{u=0}^{t-1}1_B(\omega T^{s+u})\right]\geqslant\frac{1}{L}.$$

2. Относительная частота нулей и единиц

В нашем изложении теории относительной частоты произвольных блоков мы немного отступим назад и займемся сначала только относительной частотой нулей и единиц.

Для произвольного блока $A = a_0 \dots a_{m-1}$ мы назовем

$$\rho_1(A) = \frac{1}{m} \sum_{k=0}^{m-1} a_k$$

относительной частотой единиц в A, а

$$\rho_0(A) = \frac{1}{m} \sum_{k=0}^{m-1} (1 - a_k) = 1 - \rho_1(A)$$

— *относительной частотой нулей*. Эти функции удовлетворяют следующим простым соотношениям:

$$\rho_0(A \times B) = \rho_0(A)\,\rho_0(B) + \rho_1(A)\,\rho_1(B), \tag{1}$$

$$\rho_1(A \times B) = \rho_1(A)\,\rho_0(B) + \rho_0(A)\,\rho_1(B) \tag{2}$$

(A, B — произвольные блоки). Для доказательства подсчитаем нули в $A \times B$.

Если $B = b_0 \dots b_{n-1}$, то $A \times B = A^{b_0} \dots A^{b_{n-1}}$, так что при $b_k = 0$ в A^{b_k} содержится столько же нулей, сколько в A, а при $b_k = 1$ — столько нулей, сколько в A единиц. Разделив сумму на длину блока $|A \times B| = mn$, мы получим (1). Аналогично доказывается (2).

Каждое значение относительной частоты лежит между 0 и 1, а отклонение его от $^1/_2$, взятое по модулю, — между 0 и $^1/_2$.

Определим, вообще,

$$\delta(A) = 2\left(\frac{1}{2} - \rho_0(A)\right);$$

тогда

$$\delta(A) = -2\left(\frac{1}{2} - \rho_1(A)\right)$$

и $|\delta(A)| \leqslant 1$. Докажем теперь справедливость общей формулы

$$\delta(A \times B) = -\delta(A)\,\delta(B) \tag{3}$$

(A, B — произвольные блоки). Действительно, имеем

$$\begin{aligned}\delta(A\times B)&=2\left(\frac{1}{2}-\rho_0(A\times B)\right)=\\&=2\left(\frac{1}{2}-\rho_0(A)\rho_0(B)-\rho_1(A)\rho_1(B)\right)=\\&=1-2\rho_0(A)\rho_0(B)-2(1-\rho_0(A))(1-\rho_0(B))=\\&=-1+2\rho_0(A)+2\rho_0(B)-4\rho_0(A)\rho_0(B)=\\&=-(1-2\rho_0(A))(1-2\rho_0(B))=-\delta(A)\delta(B).\end{aligned}$$

Теперь уже совсем легко построить

4.3. Пример последовательности $\omega=A\times(0P_1)\times\times(0P_2)\times\ldots$, для которой 0 и 1 не являются чезаровскими. Положим $A=0$ и потребуем, чтобы

$$\prod_{k=1}^{\infty}|\delta(0P_k)|>0, \tag{4}$$

позаботившись одновременно о сходимости ряда

$$\sum_{k=1}^{\infty}\rho_0(0P_k)$$

и необращении в нуль чисел $\delta(0P_k)$[1] ($k=1, 2, \ldots$). Все эти требования будут выполнены, если положить, например,

$$0P_k=\underbrace{1\ldots1}_{2^k-1}.$$

Тогда мы получим

$$\rho_0(0P_k)=\frac{1}{2^k} \text{ и } \delta(0P_k)=2\left(\frac{1}{2}-\rho_0(0P_k)\right)=1-\frac{1}{2^{k-1}}.$$

Из (4) следует, что

$$\lim_{n\to\infty}|\delta(0\times(0P_1)\times\ldots\times(0P_n))|=2\delta>0,$$

поэтому если

$$\omega=0\times(0P_1)\times\ldots=\omega_0\omega_1\ldots$$

[1] Последнее излишне ввиду (4). — *Прим. перев.*

и $r_n = |0\times(0P_1)\times\ldots\times(0P_n)|$, то

$$\rho_0(\omega_0\ldots\omega_{r_n-1}) = \begin{cases} \frac{1}{2}+\delta \text{ для четных } n, \\ \frac{1}{2}-\delta \text{ для нечетных } n, \end{cases}$$

так что 0 не может быть чезаровским для ω.

В частности, мы получим *примеры почти-периодических последовательностей, для которых* 0 *и* 1 *не являются чезаровскими.* Имеет место

4.4. Теорема. *Для последовательности*

$$\omega = A\times(0P_1)\times(0P_2)\times\ldots$$

0 *тогда и только тогда является чезаровским со значением*

$$\bar{1}_0(\omega) = \frac{1}{2},$$

когда выполнено одно из следующих двух условий:

1) $\rho_0(A) = \frac{1}{2}$, *либо существует* n_0, *для которого*

$$\rho_0(0P_{n_0}) = \frac{1}{2};$$

2) $\sum_{k=1}^{\infty} \min[\rho_0(0P_k),\ \rho_1(0P_k)] = \infty.$

В последнем случае 0 *является также равномерно чезаровским для* ω.

Доказательство. Обозначим для краткости

$$C_n = A\times(0P_1)\times\ldots\times(0P_n).$$

Если 0 является чезаровским для ω со значением $\bar{1}_0(\omega) = \frac{1}{2}$ и 1) не выполнено, то

$$0 \neq \delta(C_n) \to 0 \quad (n\to\infty).$$

По известиому критерию ввиду равеиства

$$|\delta(C_n)| = |\delta(A)|\prod_{k=1}^{n}|\delta(0P_k)|$$

соответствующий ряд должен расходиться:

$$\sum_{k=1}^{\infty} (1-|\delta(0P_k)|)=\infty.$$

Прн этом, однако,
$|\delta(0P_k)|=|1-2\rho_0(0P_k)|=$

$$=\left\{\begin{array}{l}1-2\rho_0(0P_k),\quad \text{если } \rho_0(0P_k)\leqslant \frac{1}{2},\\ 2\rho_0(0P_k)-1=1-2\rho_1(0P_k),\ \text{если } \rho_0(0P_k)\geqslant\frac{1}{2},\end{array}\right\}=$$
$$=1-2\min[\rho_0(0P_k),\quad \rho_1(0P_k)].$$

Отсюда следует 2). Обратно, пусть выполнено условие 1); тогда $\delta(C_n)=0$ для достаточно больших n. Если выполиено условие 2), то мы по-прежнему будем иметь

$$(5)\qquad \delta(C_n)\longrightarrow 0;$$

для этого нужно только обратить вышеприведениое рассуждение. Из соотношения (5) следует, что 0 является равномерно чезаровским для ω со значением $\bar{1}_0(\omega)=\frac{1}{2}$. Достаточно прнвести набросок доказательства: для каждого n последовательность $\omega=C_n\times(0P_{n+1})\times\ldots$ составлена из блоков C_n и C_n^1. Если t достаточно велико, то каждый отрезок

$$\omega_s\omega_{s+1}\ldots\omega_{s+t-1}$$

длины t последовательности ω можно разложить на k полных блоков C_n и C_n^1 н два «остаточных блока» (на правом и левом концах), причем суммарная длина r остаточных блоков не превосходит $2|C_n|$. Положив $|C_n|=r_n$, получим $t=kr_n+r$ и

$$\left|\rho_0(\omega_s\ \ldots\ \omega_{s+t-1})-\frac{1}{2}\right|\leqslant\frac{kr_n}{kr_n+r}\left|\rho_0(C_n)-\frac{1}{2}\right|+\frac{2r_n}{t}.$$

При $t\longrightarrow\infty$ имеем также $k\longrightarrow\infty$ и

$$\varlimsup_{t\to\infty}\left[\sup_{s\geqslant 0}\left|\rho_0(\omega_s\ldots\omega_{s+t-1})-\frac{1}{2}\right|\right]\leqslant\left|\rho_0(C_n)-\frac{1}{2}\right|=2|\delta(C_n)|.$$

Наше утверждение следует теперь из (5).

3. Относительная частота произвольных блоков

Займемся относительной частотой вхождения произвольного блока B длины $|B|>1$; при этом из-за возможных «перекрытий» между блоками трудно судить об относительных частотах вхождений в произвольный отрезок ω по относительным частотам блоков, составляющих $\omega=A\times(0P_1)\times\ldots$. Однако необходимые для этого дополнительные рассмотрения носят чисто технический характер.

4.5. Теорема. *Если для каждого $r>0$ последовательность*

$$\omega=\omega_0\omega_1\ldots$$

может быть представлена в виде

$$\omega=C\times\eta,$$

причем так, что

1) $|C|\geqslant r$,

2) 0 *является равномерно чезаровским для* $\eta=\eta_0\eta_1\ldots$ *со значением* $\bar{I}_0(\eta)={}^1/_2$,

то ω является равномерно чезаровской, причем для любого блока B

$$\bar{I}_B(\omega)=\bar{I}_{B'}(\omega).$$

Доказательство. Мы удовлетворимся наброском доказательства. Пусть B — произвольный блок и $|B|=m$. Для данного $\varepsilon>0$ возьмем r настолько большим, чтобы $\frac{m}{r}<\varepsilon$, а затем в соответствии с нашим предположением выберем C длины $|C|\geqslant r$. Увеличив в случае необходимости r, мы можем считать, что $|C|=r$.

Рассмотрим теперь представление

$$\omega=C^{\eta_0}C^{\eta_1}\ldots.$$

Для $t\geqslant 3r$ и произвольного $s\geqslant 0$ можно записать отрезок

$$\omega_s\omega_{s+1}\ldots\omega_{s+t-1}$$

в виде

$$RC^{\eta_u}C^{\eta_{u+1}}\ldots C^{\eta_{u+v-1}}S$$

с подходящими R, $u \geqslant 0$, $v > 0$, S, причем $|R|$, $|S| \leqslant r$. Если $t \to \infty$, то и $v \to \infty$. Для достаточно большого t

$$\left|\rho_0(\eta_u\eta_{u+1}\ldots\eta_{u+v-1}) - \frac{1}{2}\right| < \varepsilon$$

равномерно по s (т. е. равномерно по u).

Пусть теперь B имеет ровно b_0 вхождений в C и ровно b_1 вхождений в C^1. Среди блоков $C^{\eta_u}, \ldots, C^{\eta_{u+v-1}}$ имеется ровно $v\rho_0(\eta_u\ldots\eta_{u+v-1})$ блоков C и $v(1-\rho_0(\eta_u\ldots\eta_{u+v-1}))$ блоков C^1. Таким образом, B входит в отрезок ω, содержащий позиции s, $s+1$, $\ldots$, $s+t-1$, по крайней мере

$$b_0v\rho_0(\eta_u\ldots\eta_{u+v-1}) + b_1v\rho_1(\eta_u\ldots\eta_{u+v-1})$$

раз, причем так, что B принадлежит каждый раз одному из блоков $C^{\eta_u}, \ldots, C^{\eta_{u+v-1}}$. Кроме того, B может встречаться на каждой из границ между двумя соседними блоками C^{η_k}, перекрывая эту границу всего не более чем m раз; затем имеется не более $|R|+|S|+m \leqslant 2r$ дополнительных возможностей в начале и в конце. Мы получаем, таким образом, оценки

$$\frac{b_0v\rho_0(\eta_u\ldots\eta_{u+v-1}) + b_1v\rho_1(\eta_u\ldots\eta_{u+v-1})}{t} \leqslant \frac{1}{t}\sum_{k=0}^{t-1} I_B(\omega T^{s+k}) \leqslant$$
$$\leqslant \frac{b_0v\rho_0(\eta_u\ldots\eta_{u+v-1}) + b_1v\rho_1(\eta_u\ldots\eta_{u+v-1}) + mv + 2r}{t}.$$

Заметим теперь, что

$$t = |R| + rv + |S|, \qquad |R| + |S| < 2r.$$

Итак, левая часть нашей оценки ведет себя асимптотически при $t \to \infty$, как

$$\frac{b_0\rho_0(\eta_u\ldots\eta_{u+v-1}) + b_1\rho_1(\eta_u\ldots\eta_{u+v-1})}{r} \approx \frac{b_0+b_1}{2r},$$

а правая, — как

$$\frac{b_0+b_1}{2r} + \frac{m}{r}.$$

Так как $\frac{m}{r} < \varepsilon$ и эти утверждения справедливы равномерно по s, то доказательство закончено.

Следствием теорем 4.4 и 4.5 является

4.6. Теорема. *Последовательность*

$$\omega = A \times (0P_1) \times \ldots$$

является заведомо равномерно чезаровской со значением $\bar{1}_B(\omega) = \bar{1}_{B'}(\omega)$ (для произвольного B) *в каждом из следующих двух случаев:*

1) *существуют произвольно большие* $n > 0$, *для которых*

$$\rho_0(0P_n) = \frac{1}{2};$$

2)
$$\sum_{k=1}^{\infty} \min [\rho_0(0P_k), \ \rho_1(0P_k)] = \infty.$$

Непосредственно видно, что последовательность Морса, любая последовательность Какутани и тернарная последовательность Кини удовлетворяют условиям теоремы 4.6.

В частности, для тернарной последовательности Кини $\omega = 001001110\ldots$

$$\bar{1}_0(\omega) = \frac{1}{2} = \bar{1}_1(\omega)$$

— факт, который, возможно, будет неожиданностью для многих читателей.

§ 5. *Периодичность*

Хотя почти все наши последовательности не периодичны в строгом смысле, многие из них обладают свойствами периодичности несколько иного характера.

Для последовательности Морса, например,

$$\omega = 0110100110010110\ldots,$$

простой проверкой нетрудно установить, что множество

$$F = [0110] + [1001] + [0101] + [1010]$$

удовлетворяет соотношениям

$$\omega T^t \in F \Longleftrightarrow t \equiv 0 \pmod 2).$$

Аналогично для последовательности Кини

$$\omega' = 0010011100010011101101100\!01\ldots$$

и множества

$$F' = [001] + [110]$$

справедливо утверждение

$$\omega' T^t \in F' \Longleftrightarrow t \equiv 0 \pmod 3.$$

Предоставим читателю возможность попытаться самостоятельно найти доказательства этих утверждений. Сейчас же мы перейдем к общей теории и докажем сначала такую теорему:

5.1. Теорема. *Пусть*

$$\omega = A \times (0P_1) \times (0P_2) \times \ldots$$

и для некоторого $n \geqslant 0$

$$C_n = A \times (0P_1) \times \ldots \times (0P_n).$$

Если существует такое $j > 0$, *что в блок*

$$D = (0P_{n+1}) \times \ldots \times (0P_{n+j})$$

входит один из блоков 001, 110, 011, 100, *то для множества*

$$F = \sum_{|B| = 2\,|D|} [C_n \times B]$$

выполняется следующее утверждение:

$$\omega T^t \in F \Longleftrightarrow t \equiv 0 \pmod{|C_n|}.$$

Доказательство. Так как ω получается соединением блоков C_n и C_n^1, то в каждой позиции $t \equiv 0 \pmod{|C_n|}$ в ω входит блок вида $C_n \times B$, где $|B| = 2\,|D|$. Из сравнения $t \equiv 0 \pmod{|C_n|}$ следует, таким образом, что $\omega T^t \in F$. Так как ω получается соединением блоков $C_n \times D$ и $C_n \times D^1$, то каждый входящий в ω блок вида $C_n \times B$, где $|B| = 2\,|D|$, содержит, начиная с некоторой позиции, один из блоков $C_n C_n C_n^1$, $C_n^1 C_n^1 C_n$, $C_n C_n^1 C_n^1$, $C_n^1 C_n C_n$. Точнее, пусть $|C_n| = r$ и $\omega T^t \in F$, например $\omega T^t \in [C_n \times B]$ для подходящего B, $|B| = 2\,|D|$; пусть

$$t = kr + s, \quad 0 \leqslant s < r.$$

Тогда, скажем, блок $C_n C_n C_n^1$ входит в ωT^{kr} в позиции ir, где $i < 2\,|D| - 2$. С другой стороны, в позиции ir в

$\omega T^t = \omega T^{kr} T^s$ входит один из блоков $C_n^u C_n^v$, где $u, v = 0$ или 1. Отсюда следует, что один из блоков $C_n^u C_n^v$ входит в $C_n C_n C_n^1$ в позиции s.

Если бы s удовлетворяло неравенствам $0 < s < r$, то можно было бы рассуждать так:

C_n^u входит в $C_n C_n$ в позиции s,
C_n^v входит в $C_n C_n^1$ в позиции s.

Итак,

a) последние $r-s$ символов C_n
равны первым $r-s$ символам C_n^u,
равны первым $r-s$ символам C_n^v,
и тем самым $u = v$;

b) последние s символов C_n^u равны
первым s символам C_n,
последние s символов C_n^v равны
первым s символам C_n^1,
и тем самым $u \neq v$.

Получено противоречие, откуда следует, что $s = 0$, т. е. $t \equiv 0 \pmod{|C_n|}$. Аналогичное рассуждение можно было бы провести с блоками $C_n^1 C_n^1 C_n$, $C_n C_n^1 C_n^1$ или $C_n^1 C_n C_n$. Этим все доказано.

5.2. Теорема. *Если последовательность*

$$\omega = A \times (0P_1) \times (0P_2) \times \ldots$$

не периодична, то для каждого n найдется множество $F_n \subsetneqq \Omega$, для которого

$$\omega T^t \in F_n \Leftrightarrow t \equiv 0 \pmod{r_n},$$

где

$$C_n = A \times (0P_1) \times \ldots \times (0P_n), \quad r_n = |C_n|.$$

F есть объединение конечного числа цилиндрических множеств, содержащих вместе с каждой последовательностью ее зеркальное отражение.

Доказательство. Если ω не периодична, то последовательность $(0P_{n+1}) \times (0P_{n+2}) \times \ldots$, отличная от каждой из последовательностей $00\ldots$, $0101\ldots$, содержит один из блоков 001, 110, 001, 100 и можно применить теорему 5.1 с достаточно большим j.

В качестве упражнения стоит применить эти теоремы к последовательности Морса и тернарной последовательности Кини и сравнить результаты с утверждениями, помещенными в начале параграфа.

§ 6. Задачи

В качестве упражнения для читателя мы сформулируем несколько задач, которые примыкают к предыдущему и часть которых еще не решена (ср. Кини [5]).

1. *Однозначность представления в виде произведения.* Две последовательности блоков

$$A,\ 0P_1,\ 0P_2, \dots,$$
$$B,\ 0Q_1,\ 0Q_2, \dots$$

мы назовем эквивалентными, если найдется последовательность

$$C,\ 0R_1,\ 0R_2,\ \dots,$$

а также две последовательности $0 < m_0 < m_1 < \dots$, $0 < n_0 < n_1 < \dots$ натуральных чисел, для которых выполняются равенства

$$A = C \times \dots \times (0R_{m_0}),\ 0P_k = (0R_{m_{k-1}+1}) \times \dots \times (0R_{m_k}),$$
$$B = C \times \dots \times (0R_{n_0}),\ 0Q_k = (0R_{n_{k-1}+1}) \times \dots \times (0R_{n_k})$$
$$(k = 1,\ 2,\ \dots),$$

т. е. если они могут быть получены из некоторой третьей последовательности посредством различных разбиений скобками и перемножением элементов внутри скобок. Какие 0-1-последовательности ω обладают двумя неэквивалентными представлениями

$$A \times (0P_1) \times \dots = \omega = B \times (0Q_1) \times \dots ?$$

2. Обобщите теорему 2.4 на более широкий класс последовательностей $\omega = A \times (0P_1) \times \dots$.

3. 0-1-последовательность η называется *дочерней* относительно 0-1-последовательности ω, если «весь ее генетический материал получен от ω», т. е. если всякий входящий в η блок входит также и в ω.

a) Покажите, что последовательность ω почти-периодична тогда и только тогда, когда она является своей собственной бабушкой, и при этом относительно каждой своей дочерней последовательности, т. е. если она является дочерней последовательностью каждой своей дочерней последовательности.

b) Распространите общую теорию § 2—5 на дочерние последовательности последовательностей вида $A \times \times (0P_1) \times \ldots$. При этом необходимы некоторые изменения. В частности, проследите, какие свойства сохраняются неизменными при переходе к дочерним последовательностям.

4. Вычислите для последовательностей ω Морса и тернарной Кини относительную частоту $1_B(\omega)$ вхождения конкретных блоков, например $B=00$, 01.

5. Для последовательностей вида $\omega = \omega_0\omega_1 \ldots = A \times (0P_1) \times \ldots$ и произвольного натурального числа $d > 0$ изучите «чезаровские свойства $\operatorname{mod} d$», например существование и значение

$$\lim_{t \to \infty} \frac{1}{t} \sum_{u=0}^{t-1} 1_B(\omega T^{ud})$$

или для $\omega^{d,k} = \omega_k \omega_{k+d} \omega_{k+2d} \ldots$ существование и значение

$$\lim_{t \to \infty} \frac{1}{t} \sum_{n=0}^{t-1} 1_B(\omega^{d,k} T^n)$$

при произвольном выборе блока B.

6. Для последовательностей вида $A \times (0P_1) \times \ldots$ попытайтесь найти *все* $r_n > 1$, для которых существует хотя бы одно множество $F \subseteq \Omega$, такое, что

$$\omega T^t \in F \Leftrightarrow t \equiv 0 \pmod{r_n}.$$

7. Для произвольного 0-1-блока B определим

$r_{00}(B)$ как н. о. д. (наибольший общий делитель) номеров всех позиций, в которых в BB входит B или B^1;

$r_{01}(B)$ как н. о. д. номеров всех позиций, в которых в BB^1 встречается B или B^1;

$r(B)$ как н. о. д. чисел $r_{00}(B)$ и $r_{01}(B)$.

Блок, для которого $r_{01}(B)=|B|$, называется *полужестким*; блок, для которого $r(B)=|B|$, называется *жестким*.

a) Укажите примеры полужестких и жестких блоков.

b) Сколько % всех блоков заданной длины являются полужесткими, соотв. жесткими?

c) Модифицируйте теорему 5.1 таким образом, чтобы в ней шла речь о полужестких или жестких блоках.

d) Покажите, что

$$B\times C \text{ полужесткий} \Leftrightarrow C \text{ полужесткий},$$
$$B\times C \text{ жесткий} \Leftrightarrow C \text{ жесткий}.$$

e) Выразите $r_{00}(B\times C)$, $r_{01}(B\times C)$, $r(B\times C)$ через $r_{00}(B)$, $r_{00}(C)$, $r_{01}(B)$, $r_{01}(C)$, $r(B)$, $r(C)$, $|B|$, $|C|$.

f) Покажите, что если B входит в блок B^uB^v (u, $v=0$ или 1) в $r(B)$-й позиции, то каждый блок, входящий в B^uB^v в $kr(B)$-й позиции, входит во все B^uB^v только в позиции $kr(B)$.

8. Использованное нами множество символов $\{0, 1\}$ можно интерпретировать как циклическую группу второго порядка и записать алгебру блоков в теоретико-групповых обозначениях. Обобщите всю теорию на конечные и по возможности даже компактные группы.

ЛИТЕРАТУРА

1. Bonsdorff-Fabel-Riihimaa, Schach und Zahl, Düsseldorf, 1966.
2. Coxeter H. S. M., Unvergängliche Geometrie, Basel-Stuttgart (Birkhäuser), 1963.
3. Hedlund G., Morse M., Unending chess, symbolic dynamics and a problem in semi-groups, *Duke Math. J.*, **11** (1944), 1—7.
4. Kakutani S., Ergodic theory of shift transformations, Proc. V Berkeley Symp. Prob. Stat., vol. II, part 2 (1967), 405—414.
5. Keane M., Morse-Folgen mit vorgegebenem rationalem Spektrum, Diss. Univ. Erlangen—Nürnberg, 1967.
6. Keane M., Generalized Morse sequences, *Z. Wahrscheinlichkeitstheorie verw. Geb.*, **10** (1968), 335—353.
7. Morse M., Recurrent geodesics on a surface of negative curvature, *Trans. Amer. Math. Soc.*, **22** (1921), 84—100.
8. Speiser A., Theorie der Gruppen von endlicher Ordnung, Basel-Stuttgart (Birkhäuser), 1956.
9. Thue A., Über unendliche Zeichenreihen, Christiania Vidensk. Selsk. Skr. 1906, № 7, 22 S. Lex 8°.
10. Вейль Г., Симметрия, «Наука», М., 1968.
11*. Гильберт Д., Кон-Фоссен С., Наглядная геометрия, ОНТИ, М.—Л., 1936.
12*. Шахматный кодекс СССР, М., 1969, стр. 12—13.

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ

В указатель обозначений включены только те символы, которые состоят не из одних чисел или букв. Указаны лишь те страницы, на которых дается определение соответствующего обозначения. Символы и сокращения, допускающие алфавитное упорядочение на основе их буквенного представления, включены в предметный указатель.

ИМЕННОЙ УКАЗАТЕЛЬ

В именном указателе перечисляются лишь те страницы, на которых мы цитируем соответствующего автора. «Машина Тьюринга» не является цитатой из Тьюринга; «след.» означает, что соответствующий автор упоминается также и на следующей странице; «и др.» означает, что соответствующий автор упоминается по крайней мере на двух, но не более чем на четырех следующих страницах.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Предметный указатель симметричен в следующем смысле: если в него включен термин «атомарное заключение», то включен также и термин «заключение атомарное» с тем же списком страниц.

ОГЛАВЛЕНИЕ