Предисловие

В настоящей работе приводятся решения некоторых проблем математической логики и теории алгоритмов, использующие связь вопроса об истинности утверждений с определёнными математическими играми. Для иллюстрации рассмотрим известный пример. Пусть, дана замкнутая формула исчисления предикатов, и её предикатные символы проинтерпретированы в некоторой структуре. Нас интересует, истинна ли данная формула в данной структуре. А. Эренфойхт заметил, что с этим вопросом естественно связать игру. Для этого формула приводится к префиксному виду. Игроку, стремящемуся доказать истинность формулы, соответствуют кванторы существования; а игроку, стремящемуся доказать ложность формулы, соответствуют кванторы общности. Ходы в игре делаются в том порядке, в котором расположены кванторы формулы. Ход игрока состоит в указании какого-либо элемента структуры. В конце игры в бескванторную часть формулы вместо каждой переменной подставляется значение, которое определяется так. Если переменная x была связана квантором Q ($Q = \exists$ или $Q = \forall$), то вместо x подставляется тот элемент структуры, который был выбран игроком на ходе, соответствующем квантору Q. Если после подстановки бескванторная часть формулы становится истинной, то выиграл первый игрок; а если бескванторная часть формулы становится ложной, то выиграл второй игрок. Очевидно, что если исходная формула истинна, то у первого игрока есть выигрывающая стратегия; а если исходная формула ложна, то выигрывающая стратегия есть у второго игрока.

Заметим, что в отличие от примера из предыдущего абзаца мы будем рассматривать и игры в которых количество ходов бесконечно. Если для конечных игр просто доказать, что у одного из двух противников есть выигрывающая стратегия, то для бесконечных игр это очень нетривиальное свойство, называемое детерминированностью.

Обратимся к первой главе работы. Как известно, структура натуральных чисел со сложением и умножением имеет неразрешимую теорию первого порядка. Это обстоятельство делает особенно важным нахождение достаточно сильных разрешимых теорий. Одной из таких теорий является монадическая теория бинарного дерева. Бинарное дерево задаётся множеством всех двоичных слов и двумя операциями на нём: приписывание к слову нуля справа и приписывание к слову единицы справа. Монадическая теория состоит из формул, построенных с помощью этих двух операций, переменных по словам и по множествам слов, предиката принадлежности, пропозициональных связок и кванторов по переменным обоих типов. Наличие в языке переменных по множествам делает эту теорию очень выразительной. К ней сводятся многие интересные вопросы математической логики и теории автоматов. Один из последних примеров такого сведения недавно предложен В. Л. Селивановым в докладе, представленном в [**7**]. Там изучается круг вопросов следующего типа: "можно ли по монадической формуле (со свободными переменными) эффективно узнать, выражает ли она предикат, выразимый элементарной формулой в той же сигнатуре?".

Доказательство разрешимости монадической теории бинарного дерева было найдено М. Рабином в 1969 году [**14**]. Каждой формуле рассматриваемого языка эффективно сопоставляется конечный автомат, работающий на бинарном дереве, вершины которого размечены подходящим конечным алфавитом. Ключевым оказывается переход от автомата, распознающего какое-то множество разметок дерева, к автомату, распознающему дополнение до этого множества. Доказательство Рабина было очень сложным и, в частности, оно использовало трансфинитную индукцию по всем счётным ординалам. В докладе на международном математическом конгрессе в Ницце Рабин поставил проблему нахождения более простого доказательства, которое не использовало бы трансфинитной индукции [**15**].[1] В теореме I.1 мы предлагаем такое доказательство, основанное на играх. Оно было изложено в курсе лекций «Разрешимые теории», который был прочитан А. Л. Семёновым на кафедре математической логики Московского государственного университета в 1979/1980 учебном году. В 1981 году на той же кафедре автор защитил дипломную работу, содержащую этот результат. Соответствующая публикация автора в российском журнале "Семиотика и информатика" [**3**] была переведена международным журналом "Bulletin of the European Association for Theoretical Computer Science" [**6**].

Автор признателен Сергею Ивановичу Адяну, который посоветовал более формально выразить различие между доказательством из [**14**] и нашим доказательством, изложенным в § 2. Точные утверждения для выявления указанного различия вероятно связаны с проблемой аксиоматизации, поставленной П. С. Новиковым. Эта проблема была решена для одной функции следования в [**17**]. План решения этой проблемы для двух функций следования обсуждается в § 3.

[1]Первая из поставленных в этом докладе проблем гласила: «1. Упростить доказательство теоремы 2(*ii*), возможно, за счёт устранения трансфинитной индукции, использованной в [2]». Здесь теорема 2(*ii*) — это ключевое утверждение из рассуждения Рабина, [2] — статья [**14**] из нашего списка литературы.

Во второй главе работы рассматривается общая теория алгоритмов, то есть теория изучающая свойства алгоритмов, не зависящие от конкретных моделей вычислений. С точки зрения математической логики значительная часть этой теории может рассматриваться как теория некоторой структуры, введённой Х. Фридманом в [**10**]. Мы показываем, что для обширного класса формул истинность в этой структуре выражается посредством некоторой игры, которая не использует понятия вычислимости ([**4**]). Предлагаемая интерпретация позволяет прояснить известный в общей теории алгоритмов феномен релятивизуемости. Под релятивизацией понимается замена вычислимости на вычислимость относительно какого-то оракула. Построить истинную формулу общей теории алгоритмов, которая становится ложной при релятивизации любым невычислимым оракулом, — это просто. Тем не менее, как показывает математическая практика, релятивизации всех "естественных" истинных утверждений тоже истинны.

Третья глава работы посвящена вопросу, которым интересовались математики ещё в XVIII веке. А именно, математическому уточнению понятия случайной двоичной бесконечной последовательности. А. Н. Колмогоров в [**1**] сравнивает два способа такого уточнения. В первом способе используется введённое Колмогоровым понятие энтропии конечной двоичной последовательности. Для бесконечной двоичной последовательности α функция $K(\alpha \wr n)$ сопоставляет натуральному числу n энтропию начала α длины n. Неформально говоря, последовательность тем более случайна, чем больше значения функции K. Второй способ уточнения понятия случайности исходит из классического закона больших чисел. То есть частота нулей и единиц должна стремиться к $1/2$. Но последовательность $010101\ldots$ явно неслучайна! Может быть потребовать, чтобы закон больших чисел выполнялся для всякой подпоследовательности? Так тоже не получится, потому что можно рассмотреть подпоследовательность, состоящую как раз из тех членов начальной последовательности, которые равны нулю. Разумным компромиссом оказывается требование выполнения закона больших чисел для подпоследовательностей из достаточно широкого класса. Колмогоров в [**1**] рассмотрел класс всех подпоследовательностей, номера членов которых задаются вычислимыми монотонно возрастающими функциями. Колмогоров доказал, что для этого класса последовательности случайные в смысле второго способа уточнения бывают "максимально неслучайными" в смысле первого способа уточнения. А именно, он построил случайную в смысле закона больших чисел последовательность α, у которой $K(\alpha \wr n) = O(\log n)$. То есть энтропия начала α длины n почти так же мала, как длина двоичной записи числа n. В той же статье Колмогоров выдвинул гипотезу, что его результат можно усилить, расширив класс подпоследовательностей, для которых требуется выполнение закона больших чисел. Расширенный класс подпоследовательностей, который предложил рассмотреть А. Н. Колмогоров, полностью описан в абзаце перед определением III.1. В [**5**] автор опроверг гипотезу Колмогорова, доказав, что если $\exists \varepsilon < 1\ \exists c\ \forall n\ K(\alpha \wr n) < \varepsilon n + c$, то последовательность α неслучайна в смысле закона больших чисел. При этом используются игры с переменными ставками (как в казино).

Для удобства читателя основные понятия из теории конечных автоматов на бесконечных деревьях приведены в § 1 главы I. Что касается использования основных понятий общей теории алгоритмов (в главе II) и теории колмогоровской энтропии (в главе III), то мы следуем книге В. А. Успенского и А. Л. Семёнова [**8**].

Автор очень благодарен своему научному руководителю Алексею Львовичу Семёнову за большую поддержку в работе.

ГЛАВА I

Упрощённое доказательство теоремы Рабина о разрешимости монадической теории дерева

Изложенный в первой главе результат используется для доказательства разрешимости монадической теории дерева с двумя функциями следования. Расскажем об общем строении этого доказательства. Во-первых, язык теории удобно модифицировать так, чтобы заменить индивидные переменные на предикатные. Для этого следует вместо вершин дерева говорить об одноэлементных множествах, эти вершины содержащих. Во-вторых, набор одноместных предикатов будет отождествляться с разметкой дерева наборами значений характеристических функций. В-третьих, каждой формуле со свободными переменными эффективно сопоставляется конечный автомат. Этот автомат распознаёт в точности разметки, соответствующие тем интерпретациям свободных переменных, при которых формула становится истинной. Сопоставление автомата происходит индукцией по построению формулы. Таким образом, разрешимость теории вытекает из следующих пяти алгоритмических фактов:

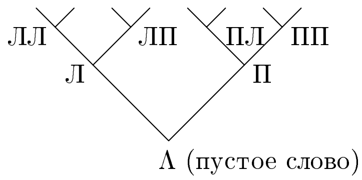
(1) можно построить автомат для распознавания области истинности атомарной формулы;
(2) по двум автоматам, распознающим какие-то множества, можно построить автомат для распознавания объединения этих множеств;
(3) по автомату, распознающему множество $(n+1)$-элементных наборов разметок, можно построить автомат для распознавания проекции этого множества на первые n координат;
(4) по автомату, распознающему какое-то множество, можно построить автомат для распознавания дополнения этого множества;
(5) по автомату можно выяснить, распознаёт ли он пустое множество.

Первые три факта устанавливаются очень просто. При этом в доказательствах фактов (2) и (3) существенно используется недетерминированность автоматов. Но именно недетерминированность оказывается основной проблемой при установлении (4). Факт (5) достаточно сложен, но проще чем (4). Факт (5) можно эквивалентно выразить на языке униформизации автоматов с одним следованием. Как раз в таком виде пятый факт установил Р. Макнотон в 1966 году [**13**]. Для этого он ввёл игровую интерпретацию, которая очень прояснила природу понятий и рассуждений. Однако рассмотренных Макнотоном игр оказалось недостаточно для установления факта (4). Первое доказательство, найденное М. Рабином в 1969 году [**14**], было не игровым и основывалось на трансфинитной индукции. В теореме I.1 мы доказываем факт (4) игровым способом, причём рассуждение становится существенно проще, чем у Рабина.

Перейдём к точным формулировкам.

§ 1. Монадическая теория двух следований и конечные автоматы на деревьях

Дадим определение монадической теории двух следований, обозначаемой $S2S$. Она состоит из всех формул определяемого далее языка, истинных в определяемой далее интерпретации. Язык содержит предметные (=индивидные) и множественные (=предикатные) переменные; его атомарными формулами являются формулы вида $x \in Q$, $\text{Л}(x,y)$, $\text{П}(x,y)$, где x, y — предметные переменные, Q — множественная переменная. В формулах языка допускаются логические связки и кванторы как по предметным, так и по множественным переменным. Чтобы описать интерпретацию, рассмотрим *бинарное дерево* конечных слов в алфавите $\{\text{Л}, \text{П}\}$:



Слова этого алфавита будем называть также вершинами дерева. Значениями предметных переменных являются вершины бинарного дерева, значениями множественных переменных — любые множества вершин. Атомарные формулы интерпретируются так: $x \in Q$ означает принадлежность вершины x множеству Q, $\text{П}(x,y)$ означает, что слово y получается из слова x приписыванием справа буквы П, аналогично понимается $\text{Л}(x,y)$. Итак, теория $S2S$ описана.

Теорема I.1. *Теория $S2S$ разрешима.*

Мы будем рассматривать вариант теории $S2S$, формулы которого содержат лишь множественные переменные, а атомарными формулами служат $P \in Q$, $\text{Vert}(P)$, $\text{П}(P,Q)$, $\text{Л}(P,Q)$. Интерпретация атомарных формул такова: $\text{Vert}(P)$ утверждает, что P — одноэлементное множество; $P \in Q$ — что P одноэлементно и его единственный элемент принадлежит Q; $\Pi(P, Q)$ и $\text{Л}(P, Q)$ — что P и Q одноэлементны, $P = \{x\}$ и $Q = \{y\}$ и выполнено $\Pi(x, y)$ (соответственно $\text{Л}(x, y)$). Очевидно, что этот вариант теории $S2S$ эквивалентен исходному с точки зрения разрешимости. Именно его в дальнейшем мы будем обозначать $S2S$.

Пусть Σ — некоторый алфавит. Будем называть Σ-деревом бинарное дерево, во всех вершинах которого расставлены буквы алфавита Σ, то есть всюду определённое отображение множества вершин в Σ. В дальнейшем мы определим понятие автомата на Σ-деревьях и понятие «автомат допускает Σ-дерево». Таким образом, каждому автомату будет соответствовать некоторое подмножество множества всех Σ-деревьев — множество допускаемых им деревьев. Получаемые таким образом подмножества будут называться *автоматными.*

Каждому множеству вершин бинарного дерева сопоставим $\{0, 1\}$-дерево, поставив в вершинах из этого множества 1, а в остальных 0. Подобным же образом каждому набору $\langle P_1, \ldots, P_n \rangle$ из n множеств вершин можно сопоставить $\{0, 1\}^n$-дерево. Будем называть множество наборов вида $\langle P_1, \ldots, P_n \rangle$ автоматным, если соответствующее множество $\{0, 1\}^n$-деревьев автоматно.

Лемма I.1. *Пусть $A(P_1, \ldots, P_n)$ — формула языка $S2S$, все параметры которой содержатся среди $P_1, \ldots, P_n$. Тогда автоматным является множество всех $\{0, 1\}^n$-деревьев, соответствующих тем наборам значений $P_1, \ldots, P_n$, при которых $A(P_1, \ldots, P_n)$ истинно в интерпретации $S2S$. Соответствующий автомат может быть эффективно указан по формуле $A(P_1, \ldots, P_n)$.*

Доказательство этой леммы ведётся индукцией по построению формулы. Главную трудность при этом представляет построение по автомату $\mathfrak{A}$ другого автомата $\mathfrak{L}$, допускающего те и только те деревья, которые не допускаются автоматом $\mathfrak{A}$. Новый способ такого построения, изложенный в § 2, и составляет основную часть главы I.

Дадим теперь некоторые определения и формулировки, связанные с конечными автоматами.

Автоматы на сверхсловах

Мы начнём с определения важного, но для нас вспомогательного понятия — понятия автомата на сверхсловах.

Пусть Σ — некоторый алфавит. *Сверхсловом* в алфавите Σ называется бесконечная последовательность букв алфавита Σ. *Автомат $\mathfrak{A}$ на сверхсловах* задаётся:

1) конечным множеством S, элементы которого называются состояниями автомата $\mathfrak{A}$; элементы $\mathcal{P}(S)$ (подмножества S) мы будем называть макросостояниями;
2) таблицей переходов — множеством $R \subset S \times \Sigma \times S$; если $\langle s, a, s' \rangle \in R$, то говорят, что автомат $\mathfrak{A}$, находясь в состоянии s и читая букву a, может перейти в состояние s';
3) множеством $S_0 \subset S$ начальных состояний;
4) некоторым множеством $F \subset \mathcal{P}(S)$; те макросостояния, которые входят в F, называются заключительными.

Если начальное состояние одно, а таблица переходов автомата является графиком всюду определённой функции из $S \times \Sigma$ в S (находясь в любом состоянии и читая любую букву, автомат может перейти ровно в одно состояние), то такой автомат называется *детерминированным.*

Пусть $\mathfrak{A}$ — автомат на сверхсловах алфавита Σ, A — сверхслово в алфавите Σ. *Ходом автомата* $\mathfrak{A}$ *на сверхслове* A называется бесконечная последовательность состояний, которая может возникнуть при чтении автоматом $\mathfrak{A}$ сверхслова $A = a_0a_1\ldots$. Ходов может быть много, а может не быть вовсе. Ясно, однако, что для детерминированного автомата ход на данном сверхслове всегда существует и единствен. Более точно, ходом называется последовательность (сверхслово) $s_0s_1\ldots$ состояний автомата $\mathfrak{A}$, в которой s_0 — начальное состояние (то есть $s_0 \in S_0$) и для каждого i автомат $\mathfrak{A}$, читая a_i и находясь в состоянии s_i, может перейти в состояние s_{i+1}. Каждому сверхслову соответствует его *предел* — множество тех символов, которые встречаются в этом сверхслове бесконечно много раз. Ход, предел которого является заключительным макросостоянием, называется *допускающим.* Говорят, что автомат $\mathfrak{A}$ *допускает* сверхслово A, если существует допускающий ход автомата $\mathfrak{A}$ на A. В противном случае говорят, что автомат $\mathfrak{A}$ *отвергает* сверхслово A. Таким образом, с каждым автоматом связано некоторое множество сверхслов, а именно множество сверхслов, допускаемых этим автоматом. Возникающие таким образом множества сверхслов называются *автоматными.* В 1962 году Р. Бюхи доказал, что любое множество сверхслов, задаваемое автоматом, может быть задано и детерминированным автоматом ([**9**]). Причём приведение автомата к детерминированной форме делается эффективно. Доказательство было упрощено Р. Макнотоном ([**13**]) с использованием игрового подхода.

Автоматы на деревьях

Деревом в алфавите Σ (или Σ-*деревом*) называется бинарное дерево, в вершинах которого стоят буквы алфавита Σ.

Автомат на Σ-деревьях задаётся:

1. Конечным набором *состояний* S с одним выделенным *начальным* состоянием. (Подмножества S мы будем, как и прежде, называть макросостояниями.)

2. Таблицей переходов — некоторым подмножеством множества $S \times \Sigma \times S \times S$. Элемент $\langle s, a, s', s'' \rangle$ из $S \times \Sigma \times S \times S$ мы будем изображать в виде схемы:

$$\underset{s,a}{{}^{s'}\bigvee^{s''}}\,.$$

Если он входит в таблицу переходов автомата $\mathfrak{A}$, то мы будем называть его *переходом* автомата $\mathfrak{A}$ и говорить, что если в некоторой вершине было состояние s и буква a, то возможно, что в следующих вершинах будут состояния s' и s''.

3. Списком *заключительных макросостояний.*

Если заданы автомат и дерево, возникает множество возможных ходов этого автомата на этом дереве. Каждый ход есть расстановка состояний во всех вершинах бинарного дерева, начинающаяся с начального состояния и согласованная с таблицей переходов. Более точно, *ход автомата* $\mathfrak{A}$ на Σ-дереве D есть S-дерево H удовлетворяющее такому условию: в корне H стоит начальное состояние и если x — любая вершина бинарного дерева, a — стоящая в ней буква дерева D, s — стоящая в x буква хода H, s' и s'' — буквы хода H стоящие в xЛ и xП, то $\langle s, a, s', s'' \rangle$ входит в таблицу переходов. Каждому ходу теперь (в отличие от автоматов на сверхсловах) соответствует много предельных макросостояний: вдоль каждого пути своё. Более точно, пусть $x_0 x_1 \ldots$ путь в бинарном дереве (то есть последовательность вершин, в которой $x_0 = \Lambda$ и x_{i+1} — одна из двух вершин, непосредственно следующих за x_i). Если выбраны ход H и путь, то возникает сверхслово в алфавите S, состоящее из букв стоящих в тех вершинах, через которые проходит путь. Предел этого сверхслова (то есть множество состояний, входящих в него бесконечно много раз) мы и будем называть *предельным макросостоянием хода вдоль выбранного пути.* Ход называется *допускающим*, если все предельные макросостояния (вдоль всех путей) заключительны.

Говорят, что автомат *допускает* дерево, если существует допускающий ход, то есть такой ход, что возникающие вдоль всех путей предельные макросостояния входят в список заключительных. В противном случае — если для всякого хода есть путь, предел вдоль которого не заключителен — говорят, что автомат *отвергает* дерево. Множество деревьев называется *автоматным*, если существует автомат, который допускает деревья из этого множества и только их. Мы говорим, что автомат *распознаёт* множество допускаемых им деревьев. Как объяснялось выше, наша цель состоит в доказательстве того, что дополнение любого автоматного множества B автоматно и что распознающий дополнение автомат может быть эффективно указан по автомату, распознающему множество B. Это доказательство и проводится в следующем параграфе.

§ 2. Доказательство теоремы об автоматности дополнения

Стратегии

Пусть $\mathfrak{A}$ — некоторый автомат на Σ-деревьях. Мы хотим построить автомат $\mathfrak{L}$, который будет допускать те и только те деревья, которые не допускает $\mathfrak{A}$. Это будет сделано в два этапа. Сначала мы введём понятие «отвергающей стратегии» для данного автомата на данном дереве. Такая стратегия будет существовать в том и только в том случае, когда автомат отвергает дерево. Затем мы построим автомат $\mathfrak{L}$, допускающий ход которого будет существовать тогда и только тогда, когда существует отвергающая стратегия. Этот автомат и будет искомым.

Отвергающая стратегия есть стратегия поиска в любом ходе данного автомата на данном дереве пути с незаключительным пределом. Такой путь ищется последовательно, начиная от корня дерева. Происходит это так. Пусть дан некоторый ход H. На первом шаге рассматривается переход, стоящий в корне и выбирается одно из направлений — левое или правое. Пусть, например, выбрано левое. Далее рассматривается переход, стоящий в ходе H в левой вершине первого уровня (вершине Л) и снова выбирается одно из направлений. Таким образом, на каждом шаге выбирается одно из направлений (в зависимости от наблюдаемого на этом шаге перехода) и осуществляется движение в этом направлении к следующей вершине. Таким образом в результате применения стратегии к ходу H в нём возникает путь. Отвергающая стратегия должна в применении к любому ходу давать путь с незаключительным пределом.

Опишем понятие стратегии более формально. Пусть зафиксирован автомат $\mathfrak{A}$ и дерево D. Рассмотрим все переходы автомата $\mathfrak{A}$, возможные в корне дерева, то есть те, которые имеют вид ${}^{s'}\bigvee^{s''}_{s,a}$, где s — начальное состояние $\mathfrak{A}$ и a — буква, стоящая в корне дерева D.

Поделим их как-то на *левые* и *правые.* Если какой-то ход H на дереве D начинается с левого (правого) перехода, то стратегия будет искать в этом ходе путь с незаключительным пределом, идущий на первом шаге налево (соответственно направо). После такого деления определяются состояния, которые можно встретить в вершине Л в процессе поиска (коротко: *возможные в* Л *состояния*, то есть состояния, стоящие слева сверху у переходов, отнесённых к левым; аналогично определяются возможные в П состояния). Заметим, что множества возможных в Л и П состояний могут быть и пустыми. Далее поделим все переходы автомата $\mathfrak{A}$, имеющие внизу возможное в Л состояние и стоящую в Л букву (*возможные в* Л *переходы*), на левые и правые. Это деление определяет, как будет стратегия искать путь с незаключительным пределом на втором шаге. После этого определяем, какие состояния возможны в вершинах ЛЛ и ЛП. Аналогичным образом мы, поделив возможные в П переходы на левые и правые, определим возможные в вершинах ПЛ и ПП состояния. И так далее.

Задать *стратегию для автомата* $\mathfrak{A}$ *на дереве* D означает решить для каждой вершины, какие возможные в этой вершине переходы отнести к левым, а какие — к правым. Заметим, что множество возможных в данной вершине состояний (и, следовательно, множество возможных в данной вершине переходов) зависит от решений, принятых стратегией на предыдущих шагах.

Итак, пусть задана стратегия для данного автомата $\mathfrak{A}$ на данном дереве D. Она, как это было описано, ищет в любом ходе автомата некоторый путь. Стратегия будет называться *отвергающей*, если отыскиваемые ей во всех ходах автомата пути имеют незаключительные пределы и, более того, всякий вероятный путь данной стратегии имеет незаключительный предел. *Вероятным путём данной стратегии* (на данном дереве для данного автомата) называется путь, который может быть получен следующим образом. Сначала мы выбираем какой-нибудь возможный в корне переход. Смотрим, левым или правым объявляет его стратегия. Пусть левым. Посмотрим, какое состояние стоит слева вверху в этом переходе. Это одно из возможных в Л состояний. Выберем возможный в Л переход, имеющий внизу рассматриваемое состояние. Смотрим, левый этот переход или правый. Пусть правый. Посмотрим, какое состояние стоит справа вверху в нём. Оно возможно в вершине ЛП. И так далее. Если этот процесс не оборвётся из-за отсутствия возможных переходов, начинающихся с данного состояния, то получится некоторый путь в дереве и расставленные вдоль него состояния. Пути, которые можно получить таким образом, и называются вероятными путями данной стратегии. Всякий путь, получающийся при применении стратегии к любому ходу автомата $\mathfrak{A}$ на дереве D, является вероятным; обратное, вообще говоря, неверно, так как вероятный путь требует выбора переходов лишь вдоль пути, и неизвестно, можно ли этот выбор продолжить до хода на всём дереве.

Итак, мы ввели понятие стратегии (для данного автомата на данном дереве) и выделили отвергающие стратегии. Существование отвергающей стратегии для $\mathfrak{A}$ на D достаточно для того, чтобы дерево D не допускалось автоматом $\mathfrak{A}$. Чтобы сделать условие необходимым, надо изменить понятие стратегии, допустив наличие в ней «памяти конечного объёма». Данное нами выше — предварительное — определение окажется частным случаем этого более общего понятия стратегии, к изложению которого мы и переходим.

Модификация понятия стратегии — стратегии с памятью

Стратегия с памятью отличается от простой стратегии тем, что при решении вопроса о том, как дальше искать в данном ходе путь с незаключительным пределом, учитывается не только переход, имеющийся в рассматриваемой вершине, но и история поиска, отражённая во «внутреннем состоянии». Дело в том, что при применении стратегии к двум различным ходам мы можем прийти в одну и ту же вершину, причём переходы, стоящие в этой вершине в обоих ходах, могут быть одинаковыми. Наличие «памяти» позволяет в одном случае пойти налево, в другом случае — направо.

Мы не вводим явно игр с конечной памятью, однако наши определения мотивируются рассмотрением игры между автоматом и стратегией.

Новое понятие стратегии определяется следующим образом. Пусть для каждого состояния s автомата $\mathfrak{A}$ фиксирован один или несколько различных *экземпляров* s_1, s_2, ... этого состояния (формально говоря, задано некоторое множество E всех экземпляров всех состояний и его наложение φ на множество S). Пусть для каждой пары состояний $\langle s, s' \rangle$ и для каждого экземпляра e состояния s задан некоторый экземпляр e' состояния s', называемый *результатом применения перемещения* $s \to s'$ *к экземпляру* e (формально говоря, задана функция $\psi\colon S \times E \to E$, для которой $\varphi(\psi(s', e)) = s'$ при всех $s' \in S$ и $e \in E$). Пусть, наконец, среди экземпляров начального состояния зафиксирован некоторый экземпляр, называемый *начальным.* В этом случае мы говорим, что задано *стратегическое множество* E *для автомата* $\mathfrak{A}$. Мы определим понятия *стратегии и отвергающей стратегии для автомата* $\mathfrak{A}$ *на дереве* D *на основе стратегического множества* E; если в E у каждого состояния будет по одному экземпляру, новое определение совпадёт со старым.

Раньше выбор стратегии определял в каждой вершине множество возможных состояний; теперь вместо него будет множество *возможных экземпляров.* (При этом один экземпляр может быть возможным, а другой экземпляр того же состояния — нет.) Пусть $\underset{s,a}{{}^{s'}\bigvee^{s''}}$ — переход автомата $\mathfrak{A}$, e — экземпляр состояния s. Рассмотрим схему вида $\underset{e,a}{{}^{e'}\bigvee^{e''}}$, где e' и e'' получаются в результате применения перемещений $s{\to}s'$ и $s{\to}s''$ к e. (Заметим, что e' и e'' являются экземплярами s' и s'' соответственно.) Все схемы такого вида (полученные из всех переходов автомата при всевозможных e) назовём *экземплярными переходами.* Экземплярные переходы, внизу которых стоит возможный в вершине x экземпляр и та же буква, что у дерева D в этой вершине, мы будем называть *возможными* в вершине x экземплярными переходами. В каждой вершине стратегия делит возможные экземплярные переходы на *левые* и *правые.* (При этом два экземплярных перехода, полученные из одного простого перехода, могут быть классифицированы по-разному.) Это деление определяет множества возможных экземпляров в следующих вершинах: к примеру, множество возможных экземпляров в вершине xЛ есть множество всех тех экземпляров, которые стоят слева вверху в возможных в вершине x переходах, объявленных левыми. В начальной вершине имеется единственный возможный экземпляр — начальный экземпляр (начального состояния).

Вероятные пути стратегии определяются как раньше, с тем изменением, что каждому пути соответствует последовательность экземпляров (а не состояний, как раньше). Однако при определении понятия *отвергающей* стратегии нас будут интересовать лишь состояния (какие экземпляры данного состояния будут встречаться, нам будет безразлично). Именно, стратегия называется отвергающей, если для каждого вероятного пути соответствующая последовательность состояний имеет незаключительный предел.

Пусть теперь помимо стратегии для автомата $\mathfrak{A}$ на дереве D на основе стратегического множества M задан ход $\mathfrak{A}$ на D. Как, применив отвергающую стратегию, найти в этом ходе путь с незаключительным пределом? Для этого нужно, идя снизу вверх, заменить состояния на их экземпляры во всех переходах (начав с начального экземпляра начального состояния).

После этого надо посмотреть, каким объявлен экземплярный переход, стоящий в корне. Пусть левым. Тогда надо сдвинуться налево и перейти в вершину Л. Стоящий там экземплярный переход является возможным и снова объявлен левым или правым. В зависимости от этого мы перейдём в вершину ЛЛ или ЛП. И так далее. Получающийся путь будет одним из вероятных и, следовательно, будет иметь незаключительный предел. Мы доказали одну из импликаций (2) $\Longrightarrow$ (1) следующего утверждения:

Утверждение 1. *Для всякого автомата $\mathfrak{A}$ существует такое конечное стратегическое множество M, что для всякого дерева D (в соответствующем алфавите) условия*

(1) *«$\mathfrak{A}$ отвергает D» и*
(2) *«существует отвергающая стратегия для $\mathfrak{A}$ на D на основе M»*

равносильны.

Наша ближайшая цель — завершить доказательство этого утверждения, показав, что при подходящем стратегическом множестве M из (1) следует (2). После этого нам останется лишь понять, что существование отвергающей стратегии для $\mathfrak{A}$ на D на основе M эквивалентно допусканию дерева D некоторым строящимся по $\mathfrak{A}$ и M автоматом.

Введение тупиков в автоматы и стратегии

Чтобы доказать утверждение 1, нам придётся обобщить его, введя в автоматы и деревья *тупики*. Пусть, помимо алфавита Σ, задано конечное множество T, не пересекающееся с Σ. Элементы его мы будем называть тупиками. Вместо Σ-деревьев мы будем рассматривать теперь $\Sigma \times \mathcal{P}(T)$-деревья, то есть деревья, в каждой вершине которых стоит некоторая буква алфавита Σ и некоторое множество тупиков. Тупики, входящие в это множество, мы будем называть тупиками, *разрешёнными в данной вершине.* С введением тупиков соответственно изменяется и определение автомата. Именно, таблица переходов автомата состоит из переходов вида

$$ {}^{u}\bigvee_{s,a}^{v}, $$

где s — состояние, a — буква алфавита Σ, а u и v принадлежат $S \cup T$ (S — множество всех состояний, T — множество всех тупиков; предполагаем, что $S \cap T = \emptyset$). Остальные компоненты автомата определяются так же, как и прежде. Определим теперь понятие хода автомата с тупиками на данном дереве. Назовём *бинарным поддеревом* непустое подмножество бинарного дерева, которое вместе с каждой вершиной содержит её предшественников и вместе с каждой вершиной содержит обоих непосредственных последователей или ни одного. *Ходом автомата с тупиками* $\mathfrak{A}$ *на* $\Sigma \times \mathcal{P}(T)$*-дереве* будет некоторое поддерево с расставленными тупиками (в вершинах без продолжений) и состояниями (в вершинах с двумя продолжениями). При этом требуется, чтобы все получающиеся переходы были переходами автомата $\mathfrak{A}$. Определение хода закончено. Ход назовём *допускающим*, если, во-первых, все его тупики разрешены (входят в $\mathcal{P}(T)$-пометку соответствующей вершины) и, во-вторых, пределы вдоль всех бесконечных путей являются заключительными макросостояниями. Будем говорить, что $\Sigma \times \mathcal{P}(T)$-дерево *допускается* автоматом с тупиками, если существует допускающий ход; в противном случае дерево *отвергается* автоматом.

Объясним теперь, что такое *стратегия и отвергающая стратегия для автомата* $\mathfrak{A}$ *на* $\Sigma \times \mathcal{P}(T)$*-дереве* D *на основе стратегического множества* M. Происходит поиск, начиная с корня, либо бесконечного пути с незаключительным пределом, либо конечного пути, ведущего в неразрешённый тупик. Рассматривая возможные экземплярные переходы, стратегия относит их к левым или к правым; новым для нас является то, что в некоторых таких переходах сверху могут быть один или два тупика. (Тупики не имеют экземпляров.) Пусть, например, в некотором возможном экземплярном переходе слева стоит тупик, а справа состояние (точнее, некоторый экземпляр некоторого состояния). Если этот переход будет объявлен правым, то в следующей справа вершине возникнет возможный экземпляр; если он будет объявлен левым, то в следующей слева вершине возникнет возможный тупик. Таким образом, в каждой вершине, помимо множества возможных экземпляров, образуется множество *возможных тупиков*. Оно состоит из тупиков, встречающихся в возможных экземплярных переходах с той стороны, к которой отнесён этот переход. *Вероятные пути* теперь будут двух сортов: бесконечные (определяемые как раньше) и конечные, упирающиеся в некоторый возможный тупик. Стратегия называется отвергающей, когда для всякой вершины возможные в ней тупики не разрешены в ней и все бесконечные вероятные пути имеют незаключительный предел. Теперь мы можем сформулировать обещанное обобщение утверждения 1.

Утверждение 1′. *Пусть дан автомат* $\mathfrak{A}$ *в алфавите* Σ *с множеством тупиков* T*. Тогда существует такое конечное стратегическое множество* M*, что для любого* $\Sigma \times \mathcal{P}(T)$*-дерева* D *условия*

(1) *«*$\mathfrak{A}$ *отвергает* D*» и*

(2) *«существует отвергающая стратегия для $\mathfrak{A}$ на D на основе M»*

равносильны.

Импликация (2) $\Longrightarrow$ (1) доказывается как раньше; импликацию (1) $\Longrightarrow$ (2) мы докажем индукцией по числу состояний автомата $\mathfrak{A}$ (число тупиков при данном числе состояний может быть любым).

Случай автомата с одним состоянием

Мы хотим доказать утверждение $1'$ для автоматов с одним состоянием (обозначаемым в дальнейшем 0) и произвольным количеством тупиков. Для такого автомата в качестве стратегического множества можно взять множество, содержащее единственный экземпляр этого единственного состояния. Мы должны доказать, что всегда имеет место одно из двух: либо существует допускающий ход, либо существует отвергающая стратегия. Рассмотрим два случая. Первый случай: макросостояние $\{0\}$ не заключительно. В этом случае предел по любому бесконечному пути не заключителен, и допускающий ход должен быть конечным. Кроме того, в определении отвергающей стратегии условие незаключительности пределов по всем бесконечным вероятным путям выполнено автоматически. В этом случае мы построим отвергающую стратегию, предположив, что допускающего хода нет. Во втором случае — когда макросостояние $\{0\}$ заключительно — все бесконечные пути имеют заключительный предел, и при построении допускающего хода достаточно проверить лишь условие, касающееся тупиков. В этом случае мы будем строить допускающий ход, предположив отсутствие отвергающей стратегии.

Первый случай: $\{0\}$ *не заключительно.*

Пусть допускающего хода нет. Это значит, что ни один переход, помещённый в корень, не может служить началом такого хода. Более точно, верна следующая

Лемма I.2. *Пусть a — буква, стоящая в корне дерева D, отвергаемого автоматом $\mathfrak{A}$.*

(а) *Если* ${}^{0}\bigvee^{0}_{0,a}$ *— переход автомата, то или поддерево с корнем в* Л*, или поддерево с корнем в* П *отвергается автоматом* $\mathfrak{A}$.

(б) *Если* ${}^{0}\bigvee^{t}_{0,a}$ *— переход автомата, то или t — неразрешённый в вершине* П *тупик, или поддерево с корнем в* Л *отвергается автоматом* $\mathfrak{A}$.

(в) *Если* $\overset{t\quad 0}{\underset{0,a}{\bigvee}}$ *— переход автомата, то или* t *— неразрешённый в* Л *тупик, или поддерево с корнем в* П *отвергается автоматом* $\mathfrak{A}$.

(г) *Если* $\overset{t\quad t'}{\underset{0,a}{\bigvee}}$ *— переход автомата, то хотя бы один из тупиков* t, t' *не разрешён в соответствующей вершине.*

(В формулировке леммы оборот «или A, или B» не исключает одновременного выполнения A и B.)

Доказательство. Лемма почти очевидна: если бы её утверждение было неверно, то можно было бы построить допускающий ход $\mathfrak{A}$, склеив его из имеющихся частей (в пункте (а), к примеру, из допускающих ходов на Л- и П-поддеревьях). $\square$

Теперь мы опишем отвергающую стратегию $\mathfrak{A}$ на D (напомним: $\mathfrak{A}$ отвергает D, $\{0\}$ — незаключительное макросостояние). На первом шаге все переходы автомата, у которых внизу стоит та же буква, что и в корне дерева, надо поделить на левые и правые. Мы делаем это так: относим переход к левым, если в нём слева стоит неразрешённый тупик или если слева стоит состояние 0 и Л-поддерево отвергается автоматом $\mathfrak{A}$. В противном случае переход относим к правым; согласно лемме 2 в нём либо справа стоит неразрешённый тупик, либо справа стоит состояние 0 и П-поддерево отвергается автоматом $\mathfrak{A}$. Из сказанного ясно, что все возможные в Л и П тупики будут неразрешёнными; ясно также, что если в какой-то из вершин Л и П будет возможно состояние 0, то поддерево с корнем в этой вершине будет отвергаться автоматом $\mathfrak{A}$. Это позволяет аналогичным образом поделить все возможные в Л и П переходы на левые и правые. Продолжая этот процесс, мы получаем отвергающую стратегию: условие с тупиками выполнено, а условие на бесконечные пути, как уже отмечалось, проверять не надо. Первый случай разобран.

Второй случай: $\{0\}$ *заключительно.*

В этом случае мы будем рассуждать в обратном направлении: предположив, что нет отвергающей стратегии, мы построим допускающий ход. Итак, пусть для автомата $\mathfrak{A}$ нет отвергающей стратегии на дереве D. Это значит, что на первом этапе некоторый переход не удалось отнести ни к левым, ни к правым так, чтобы было возможно продолжить построение стратегии. Точнее, верна следующая

Лемма I.3. *Пусть для автомата* $\mathfrak{A}$ *не существует отвергающей стратегии на дереве* D, *в корне которого стоит буква* a. *Тогда существует такой переход автомата* $\mathfrak{A}$, *что для него имеет место одна из четырёх возможностей*:

(а) *он имеет вид* $\sideset{^{0}}{^{0}}\bigvee_{0,a}$, *и ни на* Л-*поддереве, ни на* П-*поддереве нет отвергающей стратегии для* $\mathfrak{A}$;

(б) *он имеет вид* $\sideset{^{t}}{^{0}}\bigvee_{0,a}$, П-*поддерево не имеет отвергающей стратегии, а* t — *разрешённый в* Л *тупик*;

(в) *он имеет вид* $\sideset{^{0}}{^{t}}\bigvee_{0,a}$, Л-*поддерево не имеет отвергающей стратегии, а* t — *разрешённый в* П *тупик*;

(г) *он имеет вид* $\sideset{^{t}}{^{t'}}\bigvee_{0,a}$, *где* t, t' — *разрешённые в* Л *и* П *соответственно тупики.*

Доказательство. Лемма почти очевидна: если бы таких переходов не было, то каждый переход (возможный в корне) удалось бы отнести к левым или правым и продолжить этот процесс до полного построения стратегии. (Например, для перехода вида $\sideset{^{0}}{^{0}}\bigvee_{0,a}$ либо Л-поддерево, либо П-поддерево имело бы отвергающую стратегию; в зависимости от того, какое именно, мы отнесли бы этот переход к левым или правым, а затем бы действовали в соответствии с существующей отвергающей стратегией на поддереве.) $\square$

Теперь построим допускающий ход (автомата $\mathfrak{A}$ с заключительным макросостоянием $\{0\}$ на дереве D, на котором нет отвергающей стратегии). Возьмём тот переход, который существует по лемме 3. Его мы поместим в корень хода. Пусть он, к примеру, имеет вид $\sideset{^{t}}{^{0}}\bigvee_{0,a}$. Тогда t — разрешённый тупик, а на П-поддереве нет отвергающей стратегии. К поддереву можно снова применить лемму и получить следующий переход. И так далее. Получится ход, который будет допускающим: условие с тупиками выполнено, а условие с путями тривиально, так как $\{0\}$ заключительно.

На этом рассмотрение автомата с одним состоянием заканчивается.

Шаг индукции (описание стратегического множества и соответствующие леммы)

Итак, мы доказываем утверждение $1'$ для автомата $\mathfrak{A}$ с $n+1$ состоянием, считая его доказанным для автоматов с n состояниями (и произвольным количеством тупиков). Обозначим состояния автомата $\mathfrak{A}$ через $0, 1, \ldots, n$. Говоря об $(i+1)$-ом состоянии, будем считать, что $(n+1)$-ое состояние равно 0. Начальным состоянием будем считать 0.

Для доказательства введём некоторые вспомогательные автоматы. Через $\mathfrak{A}_i$ обозначим автомат, который получится из автомата $\mathfrak{A}$, если считать состояние i начальным (не меняя таблицу переходов и множество заключительных макросостояний). Через $\mathfrak{L}_i$ обозначим автомат, который получится из $\mathfrak{A}$, если считать состояние i начальным, а $i+1$ перевести в тупики. Это значит, что число состояний уменьшается на 1 (за счёт исключения $i+1$); число тупиков увеличивается на 1 (за счёт добавления $i+1$); все переходы, внизу которых стоит $i+1$, исключаются; все заключительные макросостояния, содержащие $i+1$, исключаются; а переходы, содержащие $i+1$ в верхней части, сохраняются (но $i+1$ интерпретируется как тупик, а не как состояние). Автоматы $\mathfrak{L}_i$ имеют n состояний. Согласно предположению индукции, для каждого i существует стратегическое множество M_i, удовлетворяющее такому условию: дерево D отвергается автоматом $\mathfrak{L}_i$ в том и только том случае, когда существует отвергающая стратегия для $\mathfrak{L}_i$ на D на основе M_i. Это стратегическое множество содержит в некотором количестве экземпляры всех состояний автомата $\mathfrak{L}_i$, то есть всех состояний $0, 1, \ldots, n$, кроме $i+1$. Будем считать множества M_i для разных i попарно не пересекающимися. Опишем стратегическое множество M для автомата $\mathfrak{A}$. В него входят все экземпляры, входящие во все M_i. (Таким образом, экземплярами состояния i будут все экземпляры состояния i во всех множествах M_k, в которых они есть, то есть при $i \neq k+1$.) Опишем, что мы будем называть результатом применения перемещения $i \to j$ к экземпляру e состояния i. Пусть k_0 — номер того множества M_k, в которое входит e. Если результат применения $i \to j$ к e в M_{k_0} определён (то есть $j \neq k_0 + 1$), то он и будет считаться результатом применения $i \to j$ к e в M. Если же нет (то есть $j = k_0 + 1$), результатом мы будем считать начальный экземпляр состояния j в множестве M_j. Чтобы завершить описание стратегического множества M, осталось указать в нём начальный экземпляр. Им будет начальный экземпляр состояния 0 в множестве M_0.

Построенное нами множество M и будет искомым: автомат $\mathfrak{A}$ отвергает дерево тогда и только тогда, когда существует отвергающая стратегия для $\mathfrak{A}$ на основе M. Для доказательства этого нам понадобятся две леммы, формулировки которых таковы.

Лемма I.4. *Автомат $\mathfrak{A}_i$ тогда и только тогда допускает дерево D, когда автомат $\mathfrak{L}_i$ допускает дерево D', полученное из D добавлением разрешённого тупика $i+1$ в тех вершинах x, для которых поддерево с корнем в x допускается автоматом $\mathfrak{A}_{i+1}$.*

Прежде чем формулировать следующую лемму, введём такое обозначение: M^i есть стратегическое множество M с единственным изменением — начальным экземпляром объявлен начальный экземпляр i-го состояния, имеющийся в M_i.

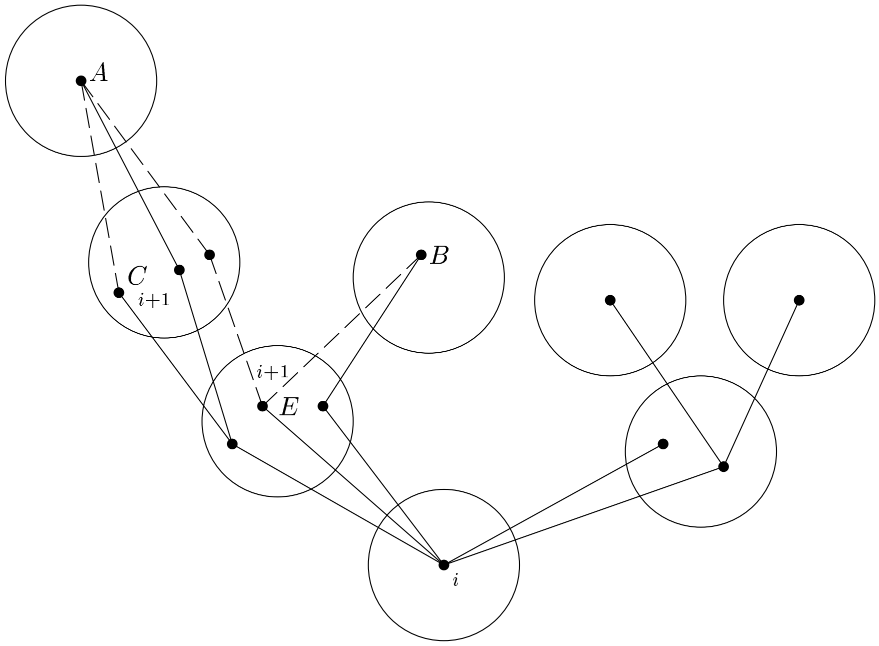
Лемма I.5. *Для автомата $\mathfrak{A}_i$ тогда и только тогда существует отвергающая стратегия на дереве D на основе M^i, когда существует отвергающая стратегия для автомата $\mathfrak{L}_i$ на основе M_i на дереве D'', получаемом из D добавлением разрешённого тупика $i+1$ в тех вершинах x, у которых на поддереве с корнем в x нет отвергающей стратегии для $\mathfrak{A}_{i+1}$ на основе M^{i+1}.*

Доказательство леммы 4. Эта лемма не касается стратегий и потому проста. Если $\mathfrak{A}_i$ допускает D, то обрезая допускающий ход там, где он попадает в состояние $i+1$, мы получим допускающий ход автомата $\mathfrak{L}_i$ на D': отрезанные части хода гарантируют разрешённость тупиков $i+1$. Наоборот, если $\mathfrak{L}_i$ имеет допускающий ход на D', то приклеивая к встречающимся в этом ходе тупикам $i+1$ допускающие ходы автомата $\mathfrak{A}_{i+1}$ (которые существуют, так как тупики $i+1$ разрешённые), мы получим ход $\mathfrak{A}_i$ на D. $\square$

Доказательство леммы 5. Эта лемма сложнее, так как относится к стратегиям. Чтобы уяснить её формулировку и понять аналогию с леммой 4, введём такую терминологию: будем говорить, что автомат квазидопускает дерево, если не существует отвергающей стратегии для этого автомата на этом дереве на основе соответствующего стратегического множества указанного в лемме. Тогда лемму можно прочесть так (перейдя к отрицаниям в обеих частях эквивалентности):

автомат $\mathfrak{A}_i$ тогда и только тогда квазидопускает дерево D, когда автомат $\mathfrak{L}_i$ квазидопускает дерево D'', полученное из D добавлением разрешённого тупика $i+1$ в тех вершинах x, для которых поддерево с корнем в x квазидопускается автоматом $\mathfrak{A}_{i+1}$.

Итак, пусть на дереве D'' существует отвергающая стратегия для автомата $\mathfrak{L}_i$ на основе M_i. А нам нужно строить отвергающую стратегию для $\mathfrak{A}_i$ на D на основе M^i. На первом шаге делим экземплярные переходы на левые и правые так же, как и в стратегии для $\mathfrak{L}_i$. Возможные на следующем шаге экземпляры будут теми же, что у стратегии для $\mathfrak{L}_i$, за одним исключением: если у стратегии для $\mathfrak{L}_i$ возможен тупик $i+1$, у нас будет возможно состояние $i+1$ (точнее, его начальный экземпляр в M_{i+1}). Но раз тупик возможен, то значит он неразрешённый; то есть на поддереве с корнем в вершине, где стоит тупик, имеется отвергающая стратегия для $\mathfrak{A}_{i+1}$ на основе M^{i+1}. Она и делит экземплярные переходы, начинающиеся с начального экземпляра состояния $i+1$.



Дальше возникает существенная проблема. Дело в том, что возможные экземпляры могут стать возможными в одной вершине по разным причинам: они могут появиться при осуществлении $\mathfrak{L}_i$-стратегии и одновременно появиться при осуществлении $\mathfrak{A}_{i+1}$-стратегии, и даже нескольких $\mathfrak{A}_{i+1}$-стратегий! На рисунке изображена одна из таких ситуаций; в кружках изображены возможные экземпляры, сплошные линии обозначают перемещения согласно $\mathfrak{L}_i$-стратегии, пунктирные — перемещения согласно $\mathfrak{A}_{i+1}$-стратегии.

В левом верхнем кружке мы видим экземпляр A, появившийся по трём причинам: в соответствии с $\mathfrak{L}_i$-стратегией, в соответствии с $\mathfrak{A}_{i+1}$-стратегией, запущенной из C, и в соответствии с $\mathfrak{A}_{i+1}$-стратегией, запущенной из E. Экземпляр B появился по двум причинам — согласно $\mathfrak{L}_i$-стратегии и согласно $\mathfrak{A}_{i+1}$-стратегии, запущенной из E. Как быть в таких случаях, какой стратегией руководствоваться? Ответ: если возможно, следует руководствоваться $\mathfrak{A}_{i+1}$-стратегиями, а среди них — запущенной как можно раньше. Это приводит к цели (построению отвергающей стратегии для $\mathfrak{A}_i$). В самом деле, условие с тупиками выполнено потому, что оно выполнено для $\mathfrak{L}_i$-стратегии и $\mathfrak{A}_{i+1}$-стратегий. Проверим условие с путями. Возьмём бесконечный вероятный путь. Либо он не попадает в зону действия $\mathfrak{A}_{i+1}$-стратегии (и тогда предел незаключительный, так как $\mathfrak{L}_i$-стратегия — отвергающая), либо, попав, уже не возвращается к $\mathfrak{L}_i$-стратегии. Единственное, что ещё может случиться — это попадание пути в зону действия другой (более ранней) $\mathfrak{A}_{i+1}$-стратегии. Но такое возможно только конечное количество раз, поэтому начиная с некоторого места путь лежит в зоне действия одной отвергающей $\mathfrak{A}_{i+1}$-стратегии и имеет незаключительный предел.

Итак, в одну сторону лемма 5 доказана. Обратная импликация гораздо проще. Пусть есть отвергающая стратегия для $\mathfrak{A}_i$ на D. Рассмотрим в ней возможные экземпляры состояния $i+1$, причём появившиеся впервые (это значит, что на каком-нибудь вероятном пути, ведущем к ним, нет экземпляров состояния $i+1$). Эти экземпляры будут начальными в M_{i+1} (таковы правила применения перемещений к экземплярам в M). Поэтому поддеревья с корнями в тех вершинах, в которых встречаются такие экземпляры, имеют отвергающую стратегию для $\mathfrak{A}_{i+1}$ на основе M^{i+1}. Следовательно, считая эти экземпляры тупиками, мы получим отвергающую стратегию для $\mathfrak{L}_i$ на D'' на основе M_i. □

Мы завершили доказательство лемм 4 и 5. На самом деле, нам в дальнейшем понадобятся лишь доказанная второй часть леммы 4 и доказанная первой часть леммы 5; обратные к ним импликации включены для полноты картины.

Завершение шага индукции

В чём польза доказанных в предыдущем пункте лемм? Если бы мы знали, что дерево D', фигурирующее в лемме 4, совпадает с деревом D'', фигурирующим в лемме 5, то мы могли бы применить индуктивное предположение к автомату $\mathfrak{L}_i$ и получить, что существование допускающего хода и отсутствие отвергающей стратегии для $\mathfrak{A}_i$ на D равносильны (чего мы и добиваемся). Однако утверждение $D' = D''$ как раз и означает, что наличие допускающего хода и отсутствие отвергающей стратегии равносильны для автомата $\mathfrak{A}_{i+1}$, который имеет столько же состояний, сколько у $\mathfrak{A}_i$. Тем не менее польза от доказанных лемм всё-таки есть.

Как и для основания индукции, мы разберём два случая: в первом из них множество S всех состояний будет заключительным, во втором — нет.

Первый случай. Множество всех состояний заключительно. Докажем, что если на дереве D нет отвергающей стратегии для $\mathfrak{A}_0$, то есть допускающий ход для $\mathfrak{A}_0$. Раз на D нет отвергающей стратегии для $\mathfrak{A}_0$, то на дереве D'' (построенном как в лемме 5) есть допускающий ход автомата $\mathfrak{L}_0$ (ведь для $\mathfrak{L}_0$ отсутствие стратегии и существование хода равносильны по предположению индукции). Чем ход $\mathfrak{L}_0$ отличается от хода $\mathfrak{A}_0$? В некоторых местах он приходит в разрешённые на D'' тупики 1. Поддеревья с корнями в этих вершинах не имеют отвергающей стратегии для $\mathfrak{A}_1$ и, значит, имеют ход для $\mathfrak{L}_1$, который станет допускающим после добавления в некоторые вершины тупиков 2. Но в этих местах можно запустить ход автомата $\mathfrak{L}_2$ и так далее. Склеивая все эти ходы, получаем ход автомата $\mathfrak{A}_0$. Он будет допускающим: каждый путь либо лежит с некоторого места в ходе одного из $\mathfrak{L}_i$ (и поэтому кончается разрешённым на дереве D тупиком или имеет заключительный предел), либо переходит бесконечное количество раз из $\mathfrak{L}_0$ в $\mathfrak{L}_1$, из $\mathfrak{L}_1$ в $\mathfrak{L}_2$, ..., из $\mathfrak{L}_n$ в $\mathfrak{L}_0$, ... и так далее по кругу — и имеет в качестве предела множество всех состояний, которое по нашему предположению заключительно. Первый случай рассмотрен.

Второй случай. Множество всех состояний не заключительно. Это случай более сложный; именно здесь будет использована структура построенного нами стратегического множества M. Мы предположим отсутствие допускающего хода и докажем наличие отвергающей стратегии. Итак, пусть на дереве D нет допускающего хода автомата $\mathfrak{A}_0$. Согласно лемме 4, на дереве D', получаемом из D добавлением в некоторых местах тупика 1, нет допускающего хода автомата $\mathfrak{L}_0$ и по предположению индукции есть отвергающая стратегия для $\mathfrak{L}_0$. Чем она отличается от $\mathfrak{A}_0$-стратегии? В $\mathfrak{L}_0$-стратегии в некоторых местах есть возможные тупики 1, а при построении $\mathfrak{A}_0$-стратегии в этих же местах возникают возможные экземпляры состояния 1 (начальные в M_1 экземпляры). Как быть с ними? Они появляются только в тех вершинах, поддерево с корнем в которых не имеет допускающего хода для $\mathfrak{A}_1$. Можно ещё раз применить лемму 4 и установить, что после соответствующего добавления тупиков 2 получаются деревья, на которых нет допускающих ходов для $\mathfrak{L}_1$ и есть отвергающие стратегии для $\mathfrak{L}_1$. Используя эти отвергающие стратегии, можно продолжить построение $\mathfrak{A}_0$-стратегии. Заметим, что спорных случаев (подобных рассмотренным в доказательстве леммы 5) здесь пока не возникает, так как $\mathfrak{L}_0$-стратегия касается экземпляров из M_0, а $\mathfrak{L}_1$-стратегия — экземпляров из M_1. Продолжая этот процесс, мы запустим стратегии для $\mathfrak{L}_2, \ldots, \mathfrak{L}_n$; стратегию для $\mathfrak{L}_{k+1}$ мы запускаем в тех местах, где у стратегии для $\mathfrak{L}_k$ появились возможные тупики $k+1$: в этих местах не существует допускающего хода для $\mathfrak{A}_{k+1}$. В некоторый момент круг замыкается и придётся снова включать $\mathfrak{L}_0$-стратегию, затем $\mathfrak{L}_1$-стратегию и так далее. Теперь уже может возникнуть вопрос: какой из различных стратегий для $\mathfrak{L}_i$ пользоваться? Ответ: той, которая запущена раньше. Проверим, получится ли действительно отвергающая стратегия для $\mathfrak{A}_0$. Условие с тупиками, очевидно, выполнено. Проверим условие с путями. Все вероятные пути делятся на два класса: либо путь, начиная с некоторого места, перемещается по экземплярам одного и того же стратегического множества M_i, либо перемещается бесконечное количество раз из одного стратегического множества (M_j) в следующее (M_{j+1}). Путь из первого класса, начиная с некоторого места, следует стратегиям для $\mathfrak{L}_i$. Переключение из зоны действия одной из них в зону действия другой возможно, если вторая начала работать раньше; поэтому такие переключения возможны только конечное количество раз. Начиная с некоторого места, путь совпадает с вероятным путём одной стратегии для $\mathfrak{L}_i$ и имеет незаключительный предел. Путь из второго класса, переключаясь из M_j в M_{j+1}, попадает в начальный экземпляр M_{j+1}; поэтому его предел — множество всех состояний, которое по нашему предположению незаключительно.

Итак, случай незаключительности множества всех состояний разобран, и индуктивное доказательство утверждения $1'$ тем самым завершено. Таким образом, мы доказали и утверждение 1. Отметим, что стратегическое множество и соответствующие ему функции φ и ψ построены по автомату эффективно. С этого момента мы можем забыть про тупики — они играли лишь вспомогательную роль, обеспечивая возможность индукции.

Завершение доказательства теоремы о дополнении

В соответствии с объявленным планом нам осталось доказать следующее

Утверждение 2. *Пусть Σ — алфавит, $\mathfrak{A}$ — автомат на Σ-деревьях (безо всяких тупиков!), M — стратегическое множество. Тогда множество Σ-деревьев, на которых существует отвергающая стратегия для $\mathfrak{A}$ на основе M, автоматно.*

Для доказательства введём понятия *слабого автомата* и *полуавтомата* на Σ-деревьях. Слабый автомат отличается от автомата только тем, что может иметь несколько начальных состояний. Полуавтомат задаётся набором состояний S с выделенным поднабором начальных состояний, таблицей переходов (всё перечисленное такое же, как у слабого автомата на Σ-деревьях), а также некоторым автоматом $\mathfrak{F}$ на S-сверхсловах. Ход полуавтомата определяется так же, как для слабых автоматов, а допускающим он называется в том случае, когда все пути, рассматриваемые как последовательности состояний, отвергаются автоматом $\mathfrak{F}$. Допускаемые полуавтоматами (слабыми автоматами) множества деревьев назовём *полуавтоматными (слабо автоматными)*. Ясно, что всякое автоматное множество полуавтоматно. Следующие две леммы показывают, что верно и обратное.

Лемма I.6. *Каждое полуавтоматное множество слабо автоматно.*

Доказательство. Автомат $\mathfrak{F}$, входящий в состав какого-то полуавтомата $\mathfrak{L}$, можно считать детерминированным. После этого несложно построить слабый автомат, эквивалентный полуавтомату $\mathfrak{L}$; в качестве множества его состояний следует взять произведение множеств состояний $\mathfrak{L}$ и $\mathfrak{F}$; ход его будет фактически состоять из хода $\mathfrak{L}$ и ходов $\mathfrak{F}$ на сверхсловах (буквами которых будут состояния $\mathfrak{L}$), возникающих вдоль всех путей. К переходам слабого автомата относятся схемы, у состояний которых первые проекции соответствуют переходу полуавтомата, а вторые проекции соответствуют переходам автомата на сверхсловах. Множество состояний слабого автомата заключительно, когда его вторая проекция является незаключительным макросостоянием в $\mathfrak{F}$. Для установления того, что построенный слабый автомат действительно эквивалентен $\mathfrak{L}$, надо воспользоваться следующим фактом. Пусть H — ход слабого автомата, а H_2 — вторая проекция H. Состояние автомата $\mathfrak{F}$ принадлежит пределу H_2 вдоль какого-то пути тогда и только тогда, когда в паре с каким-нибудь состоянием полуавтомата оно принадлежит пределу H вдоль того же пути. □

Лемма I.7. *Каждое слабо автоматное множество автоматно.*

Доказательство. Пусть дан слабый автомат, построим эквивалентный ему автомат. Состояниями автомата будут все состояния слабого автомата и одно новое состояние s_0, которое объявляется начальным. Переходами автомата будут все переходы слабого автомата и все схемы вида ${}^{s'}\bigvee^{s''}_{s_0,a}$, для которых в слабом автомате есть начальное состояние s и переход ${}^{s'}\bigvee^{s''}_{s,a}$. Множество состояний автомата объявляется заключительным тогда и только тогда, когда оно является заключительным макросостоянием в слабом автомате. Эквивалентность исходного слабого автомата и построенного автомата очевидна. □

Теперь нам осталось доказать полуавтоматность множества деревьев, на которых существует отвергающая стратегия для $\mathfrak{A}$ на основе M. Понятие стратегии просто сформулировать в виде допускающего хода некоторого полуавтомата. При этом произвол в делении экземплярных переходов на левые и правые соответствует возможности по-разному продолжать ход. Состояниями полуавтомата можно считать пары непересекающихся множеств экземплярных переходов (члены пары соответствуют множествам левых и правых экземплярных переходов). Автомат $\mathfrak{F}$ будет выискивать пути, не удовлетворяющие определению отвергающей стратегии (то есть вероятные пути с заключительными пределами). То, что автомат $\mathfrak{F}$ отвергает последовательности состояний полуавтомата вдоль всех путей, как раз означает, что стратегия действительно отвергающая.

Отметим, что моделирование отвергающей стратегии полуавтоматом, моделирование полуавтомата слабым автоматом и моделирование слабого автомата обычным автоматом произведены эффективно.

Таким образом, мы доказали утверждение 2, а вместе с тем и теорему об автоматности дополнения к автоматному множеству. При этом по автомату, распознающему какое-то множество Z, эффективно строится автомат, распознающий дополнение до Z.

§ 3. Об аксиоматизации $S2S$

Существует естественный алгоритм, который по автомату на $\{0,1\}^n$-деревьях строит формулу теории $S2S$ с n свободными предикатными переменными так, что эта формула истинна в точности на деревьях, допускаемых этим автоматом. Поэтому обоснование пяти алгоритмических фактов, приведённых в начале главы, эквивалентно доказательству некоторых формул теории $S2S$. Можно ли содержательные рассуждения, применяемые в доказательствах этих формул, перевести на язык $S2S$? Если бы ответ был положительным, можно было бы надеяться получить естественную аксиоматизацию $S2S$.

Один из основателей российской школы математической логики и теории алгоритмов Пётр Сергеевич Новиков выдвинул в 1960-е годы такую гипотезу. Рассмотрим монадическую теорию одной функции следования на натуральном ряде ($S1S$) с одноместным функциональным символом $'$ и константой 0. Все истинные формулы этой теории могут быть выведены по правилу заключения из подстановок в формулы, выводимые в исчислении предикатов первого порядка с равенством, и следующих аксиом:[1]

[1] малые буквы обозначают натуральные числа, большие буквы обозначают множества натуральных чисел

$$\forall x\ x' \neq 0,$$
$$\forall x, y\ (x' = y' \implies x = y),$$
$$\forall P\ ((P(0)\ \&\ \forall x\ (P(x) \implies P(x'))) \implies \forall x\ P(x)),$$
$$\forall y_1, \ldots, y_n, Y_1, \ldots, Y_k \exists P \forall x\ (P(x) \iff \Phi(x, y_1, \ldots, y_n, Y_1, \ldots, Y_k)),$$
где Φ — любая формула со свободными переменными $x, y_1, \ldots, y_n$, $Y_1, \ldots, Y_k$. Эта гипотеза была доказана в [**17**]. Для указанных аксиом просто строятся их аналоги в теории двух следований. Получается ли при этом полная аксиоматизация $S2S$? Мы думаем, что ответ отрицателен, и приведём формулу, которую по нашему предположению нельзя вывести. Это частный случай аксиомы выбора.

Назовём вершину выделенной, если она имеет вид Л^{m}П. Семейство всех выделенных вершин просто выразимо в $S2S$. Множество всех продолжений одной выделенной вершины будем называть выделенным конусом. Искомая формула утверждает, что *для любого множества M, пересекающегося с каждым выделенным конусом, существует множество $Q \subset M$, пересечение которого с каждым выделенным конусом одноэлементно.*

Понятно, что приведённая формула истинна. Для её доказательства в аксиоматической теории множеств даже не нужна аксиома выбора, так как вершину в непустом подмножестве конуса можно выбрать “конструктивно”. Например, можно взять самые низкие вершины множества, а среди них самую левую (самые низкие вершины имеют одинаковую высоту, их количество конечно). Однако это рассуждение нельзя провести в $S2S$, так как в монадической теории дерева нельзя выразить отношение «высота вершины x меньше высоты вершины y».

Анализ наших доказательств из предыдущего параграфа показывает, что аксиоматизация $S2S$ может быть получена из естественных аналогов аксиом для $S1S$ и некоторого варианта аксиомы выбора. Мы применяли аксиому выбора, когда “склеивали” ходы вспомогательных автоматов в ход основного автомата. Дело в том, что каждый ход вспомогательного автомата определён, вообще говоря, неоднозначно.

Первоначальное рассуждение Рабина из [**14**] не даёт искомую аксиоматизацию потому, что в нём использовано понятие фундированных функций, отображающих вершины дерева во множества вершин. Это понятие не выразимо на языке $S2S$.

ГЛАВА II

Характеризация релятивизуемых утверждений общей теории алгоритмов в игровых терминах

Вычислительная структура

В 1969 году Х. Фридман предъявил логическую структуру, подходящую чтобы утверждения общей теории алгоритмов соответствовали истинности формул того или другого языка в этой структуре [**10**].

Носителем предлагаемой структуры является любой ансамбль конструктивных объектов N, а сигнатура состоит из единственного двуместного функционального символа F, интерпретируемого как универсальная функция некоторой вычислимой главной нумерации всех частичных вычислимых функций из N в N. Структура $\langle N, F\rangle$ такого типа называется *вычислительной структурой* и является основным объектом изучения во второй главе нашей работы. Термы определяются обычным образом индуктивно. Атомарные формулы элементарного языка — это равенства термов. При интерпретации значение терма может быть не определено для тех или иных значений параметров. Атомарная формула элементарного языка истинна в данной интерпретации на определённом наборе параметров тогда и только тогда, когда значения входящих в неё термов определены для этого набора параметров и равны в данной интерпретации. Все функции в этой части работы являются, вообще говоря, частичными. Мы будем отождествлять нумерацию одноместных функций и универсальную функцию этой нумерации.

В математической логике структуры, как правило, рассматриваются с точностью до их изоморфизма (то есть биекции носителей, сохраняющей сигнатурные отношения), так как в любом логическом языке теории изоморфных структур совпадают, что доказывается индукцией по построению формул языка. Как доказал Фридман, любые две вычислительные структуры изоморфны. Отличие теоремы Х. Фридмана от известной теоремы Х. Роджерса 1958 года о вычислимом изоморфизме главных нумераций состоит в том, что изоморфизм в теореме Роджерса переставляет только номера одноместных вычислимых функций, тогда как изоморфизм вычислительных структур затрагивает и номера функций, и их аргументы, и их значения.

Теорема Фридмана. *Пусть $\langle \mathbb{N}, F\rangle$ и $\langle \mathbb{N}, G\rangle$ — две вычислительные структуры на натуральных числах. Тогда существует вычислимый изоморфизм $\langle \mathbb{N}, F\rangle$ на $\langle \mathbb{N}, G\rangle$.*

Доказательство. Нам нужно построить такую вычислимую биекцию $l\colon \mathbb{N} \to \mathbb{N}$, что выполнено

$$F(x,y) = z \iff G(l(x), l(y)) = l(z)$$

или, что равносильно, при всяком x из $\mathbb{N}$

$$F_x = l^{-1} \circ G_{l(x)} \circ l.$$

Для этого по номеру всякой вычислимой функции $h\colon \mathbb{N} \to \mathbb{N}$ мы эффективно построим некоторую биекцию $k\colon \mathbb{N} \to \mathbb{N}$ такую, что при всех x

$$h \circ F_x = G_{k(x)} \circ h.$$

Теорема о неподвижной точке даёт тогда возможность получить функцию k, совпадающую с h.

Построение k по h. Легко видеть, что по h можно эффективно построить вычислимую функцию i, которая окажется обратной к функции h, если h была биекцией. Так как F и G — универсальные функции главных вычислимых нумераций, можно эффективно найти всюду определённые вычислимые функции u и v, для которых

$$F_{u(x)} = i \circ G_x \circ h, \qquad G_{v(x)} = h \circ F_x \circ i.$$

Биекция k строится “челночным способом”: на чётных шагах мы определяем $k(m)$ для очередного m, ещё не попавшего в область определения k; на нечётных шагах мы определяем $k^{-1}(n)$ для очередного n, ещё не попавшего в область значений k. Именно, $k(m)$ мы принимаем равным $v(m)$, если $v(m)$ ещё не встречается среди уже определённых значений функции k; если же это не так, то отыскиваем такое p, которое не встречается среди этих значений и для которого $G_p = G_{v(m)}$. Мы воспользовались тем фактом, что в главной нумерации у каждой функции имеется бесконечно много номеров и по любому номеру функции можно эффективно указать сколько угодно номеров той же функции. При этом множество номеров, которые мы должны избежать , конечно. (Это рассуждение используется также в доказательстве теоремы Роджерса о вычислимом изоморфизме главных нумераций [**16**].) Аналогичным образом $k^{-1}(n)$ определяется как $u(n)$ или какое-то другое q, для которого $F_q = F_{u(n)}$ и на котором функция k ещё не определена.

Если исходная функция h была биекцией, то $i = h^{-1}$ и $G_{k(x)} = h \circ F_x \circ h^{-1}$. □

Релятивизованные вычислительные структуры

Как и все естественные утверждения общей теории алгоритмов, теорема Фридмана релятивизуема.

Назовём *вычислительной структурой с оракулом* $\boldsymbol{A}$ (или $\boldsymbol{A}$-*вычислительной структурой*) структуру, определение которой получается из определения вычислительной структуры заменой всюду вычислимости на вычислимость с оракулом $\boldsymbol{A}$ ($\boldsymbol{A}$-вычислимость). Заменяя всюду в доказательстве теоремы Фридмана вычислимость на $\boldsymbol{A}$-вычислимость, мы получим доказательство теоремы об изоморфизме для $\boldsymbol{A}$-вычислительных структур. Более того, тип изоморфизма вычислительной структуры с оракулом определяется степенью неразрешимости оракула.

Теорема II.1. *Пусть,* $\langle \mathbb{N}, F \rangle$ *— вычислительная структура с оракулом* $\boldsymbol{A}$*, а* $\langle \mathbb{N}, G \rangle$ *— вычислительная структура с оракулом* $\boldsymbol{B}$*. Тогда существование изоморфизма между* $\langle \mathbb{N}, F \rangle$ *и* $\langle \mathbb{N}, G \rangle$ *равносильно тому, что* $\boldsymbol{A}$ *и* $\boldsymbol{B}$ *эквивалентны по Тьюрингу.*

Доказательство. Пусть $\boldsymbol{A} \underset{T}{\equiv} \boldsymbol{B}$. Назовём $\boldsymbol{A}$-нумерацией $\boldsymbol{A}$-вычислимую нумерацию одноместных $\boldsymbol{A}$-вычислимых функций. Тогда каждая $\boldsymbol{A}$-нумерация является $\boldsymbol{B}$-нумерацией и наоборот, в частности, F — это $\boldsymbol{B}$-нумерация. Покажем, что F является главной $\boldsymbol{B}$-нумерацией. Действительно, пусть H — произвольная $\boldsymbol{B}$-нумерация. Тогда H является и $\boldsymbol{A}$-нумерацией, следовательно существует $\boldsymbol{A}$-вычислимая всюду определённая функция φ такая, что $\forall n \; F_{\varphi(n)} = H_n$. Функция φ одновременно является и $\boldsymbol{B}$-вычислимой функцией, сводящей $\boldsymbol{B}$-нумерацию H к $\boldsymbol{B}$-нумерации F. Таким образом, F является главной $\boldsymbol{B}$-нумерацией, а $\langle \mathbb{N}, F \rangle$ оказывается вычислительной структурой с оракулом $\boldsymbol{B}$. Релятивизованный вариант теоремы Фридмана даёт существование требуемого изоморфизма.

Обратно, пусть биекция ν осуществляет изоморфизм между $\langle \mathbb{N}, F \rangle$ и $\langle \mathbb{N}, G \rangle$. Покажем как, имея возможность определять принадлежность элемента к множеству $\boldsymbol{A}$, указать способ определять принадлежность элемента к множеству $\boldsymbol{B}$.

Пусть, α — номер в нумерации G той функции, которая увеличивает каждое число на 1. Пусть, β — номер в нумерации G характеристической функции множества $\boldsymbol{B}$. Для всякой функции $S\colon \mathbb{N} \to \mathbb{N}$ через $(S)^n$ мы будем обозначать n-ую итерацию функции S, то есть $\underbrace{S \circ \ldots \circ S}_{n \text{ раз}}$.

Имеем $n \in \boldsymbol{B} \iff G_\beta((G_\alpha)^n(0)) = 1 \iff F_{\nu(\beta)}((F_{\nu(\alpha)})^n(\nu(0))) = \nu(1)$. Так как $\nu(\beta)$, $\nu(\alpha)$, $\nu(0)$, $\nu(1)$ — константы, то последнее равенство даёт $\boldsymbol{A}$-вычислимый способ проверки принадлежности элемента к множеству $\boldsymbol{B}$. $\square$

Элементарная теория класса структур одной и той же сигнатуры — это множество замкнутых формул языка первого порядка, истинных в каждой из структур этого класса. Элементарную теорию структуры $\langle \mathbb{N}, \rho \rangle$, где ρ — некоторая сигнатура, мы будем обозначать через $\mathrm{Th}\langle \mathbb{N}, \rho \rangle$.

Как вытекает из теоремы II.1, если $\boldsymbol{A} \underset{T}{\equiv} \boldsymbol{B}$, то элементарные теории $\boldsymbol{A}$-вычислительной и $\boldsymbol{B}$-вычислительной структур совпадают. Поэтому можно говорить об элементарной теории степени неразрешимости оракула. Как будет доказано ниже, элементарные теории достаточно больших степеней совпадают (второе следствие к теореме II.5).

Теорема II.2. *Элементарная теория вычислительной структуры $\langle \mathbb{N}, F \rangle$ m-эквивалентна теории $\mathrm{Th}\langle \mathbb{N}, +, \times \rangle$. Теория $\mathrm{Th}\langle \mathbb{N}, +, \times \rangle$ m-сводится к теории любого непустого класса вычислительных структур с оракулами.*

Доказательство. Как известно, график вычислимой функции (в частности, F) выразим формулой первого порядка в структуре $\langle \mathbb{N}, +, \times \rangle$. Это даёт m-сведение $\mathrm{Th}\langle \mathbb{N}, F \rangle$ к $\mathrm{Th}\langle \mathbb{N}, +, \times \rangle$.

Покажем, что имеется не зависящее от оракула m-сведение $\mathrm{Th}\langle \mathbb{N}, +, \times \rangle$ к элементарной теории вычислительной структуры $\langle \mathbb{N}, F \rangle$ с любым оракулом. (Далее этот оракул считается фиксированным.) Выделим шесть переменных x_0, x_1, x_2, x_3, x_4, x_5, которые будут аналогами числа 0 и F-номеров следующих функций: прибавление единицы, два проектирования для функции спаривания, сложение и умножение. Запишем теперь некоторые свойства этих функций, выразимые в языке $\mathrm{Th}\langle \mathbb{N}, F \rangle$. Выражение $\exists!$ будет обозначать «существует и единственно». Для функций с номерами x_2, x_3 мы напишем аксиому спаривания

$$\forall u \, \forall y \, \exists! z \, (F_{x_2}(z) = u \ \& \ F_{x_3}(z) = y).$$

Имея функции проектирования π_1 и π_2, мы можем в сигнатуре F, π_1, π_2 говорить о многоместных вычислимых относительно оракула функциях; в частности, мы можем говорить о свойствах аналогов сложения и умножения как о свойствах подходящих одноместных функций. Это даёт алгоритм, позволяющий по формуле Φ в сигнатуре $0, ', +, \times$ строить аналогичную формулу Φ^* в сигнатуре $F, x_0, x_1, x_2, x_3, x_4, x_5$, используя в качестве аналога числа 0 число x_0, в качестве аналогов функций $'$, $+$, $\times$ функции с номерами x_1, x_4, x_5 и в качестве функций проектирования функции с номерами x_2, x_3. Формула Φ^* будет называться переводом формулы Φ. Построим таким способом переводы аксиом Пеано без аксиом индукции. Конъюнкцию полученных формул языка $\mathrm{Th}\langle\mathbb{N}, F\rangle$ с аксиомой спаривания обозначим через A. Формула A в сигнатуре F содержит шесть свободных переменных $x_0, x_1, x_2, x_3, x_4, x_5$.

Под перечислимым множеством в $\langle\mathbb{N}, F\rangle$ мы будем понимать область определения одноместной функции, имеющей номер в нумерации F. Аксиомой индукции $I(x_0, x_1)$ для числа x_0 и функции с номером x_1 в $\langle\mathbb{N}, F\rangle$ назовём следующее утверждение «каждое перечислимое множество в $\langle\mathbb{N}, F\rangle$, содержащее x_0 и вместе с каждым z содержащее $F_{x_1}(z)$, совпадает с $\mathbb{N}$». Формулу $A \mathbin{\&} I(x_0, x_1)$ обозначим через Π.

Пусть Ψ — замкнутая формула языка $\mathrm{Th}\langle\mathbb{N}, +, \times\rangle$ и $\bar{x} = x_0, x_1, x_2, x_3, x_4, x_5$. Тогда

$$\langle\mathbb{N}, +, \times\rangle \models \Psi \iff \langle\mathbb{N}, F\rangle \models \exists\bar{x}\,(\Psi^*(\bar{x}) \mathbin{\&} \Pi(\bar{x})).$$

Действительно, если $\langle\mathbb{N}, +, \times\rangle \models \Psi$, то взяв в качестве x_0 число 0 и в качестве $x_1, \ldots, x_5$ номера соответствующих арифметических функций, убедимся что $\langle\mathbb{N}, F\rangle \models \exists\bar{x}\,(\Psi^*(x) \mathbin{\&} \Pi(\bar{x}))$.

Наоборот предположим, что при фиксированных $x_0, \ldots, x_5$ $\langle\mathbb{N}, F\rangle \models \Psi^*(\bar{x}) \& \Pi(\bar{x})$. Пусть f_1, f_2, f_3, f_4, f_5 это функции, имеющие в рассматриваемой вычислительной структуре номера x_1, x_2, x_3, x_4, x_5. Истинность формулы Π в $\langle\mathbb{N}, F\rangle$ обеспечивает, что отображение $n \to (f_1)^n(x_0)$ осуществляет изоморфизм структуры $\langle\mathbb{N}, 0,', +, \times\rangle$ со структурой $\langle\mathbb{N}, x_0, f_1, f_4, f_5\rangle$. Поэтому $\langle\mathbb{N}, F\rangle \models \Psi^*(\bar{x}) \implies \langle\mathbb{N}, 0,', +, \times\rangle \models \Psi$. $\square$

Пример нерелятивизуемой формулы

Моделирование арифметики сложения и умножения в языке $\mathrm{Th}\langle\mathbb{N}, F\rangle$ даёт возможность построить в этом языке нерелятивизуемое утверждение.

Теорема II.3. *Существует замкнутая формула языка* $\mathrm{Th}\langle\mathbb{N}, F\rangle$, *ложная во всякой* $\boldsymbol{A}$*-вычислительной структуре* $\langle\mathbb{N}, F\rangle$ *с неразрешимым оракулом* $\boldsymbol{A}$ *и истинная в вычислительной структуре без оракула.*

Доказательство. Пусть, $G_y(z)$ — вычислимая главная нумерация одноместных вычислимых функций без оракула. Пусть, $B(y, z, u)$ — формула в языке $\mathrm{Th}\langle\mathbb{N}, 0,', +, \times\rangle$, выражающая предикат $G_y(z) = u$. Определённые в доказательстве предыдущей теоремы операция перевода и формула $\Pi(\bar{x})$ пригодятся нам и сейчас. Формула, которую мы ищем, выглядит так:

$$\exists \bar{x}\ \big(\Pi(\bar{x})\ \&\ \forall v \exists y\ \forall z, u\ (F_v(z) = u \iff B^*(y, z, u; \bar{x}))\big)$$

(напомним, что при переводе формулы в ней появляются новые свободные переменные $x_0, x_1, x_2, x_3, x_4, x_5 = \bar{x}$). Указанная формула выражает тот факт, что все одноместные функции, содержащиеся в нумерации F, содержатся и в нумерации G. □

Игровая интерпретация

Свяжем с замкнутой формулой Φ в сигнатуре вычислительной структуры игру $P(\Phi)$ с двумя симметричными участниками I и II. В этой игре используются два непересекающихся ансамбля конструктивных объектов X_1 и X_2. Обозначим $X_1 \cup X_2$ через X. Игроки, делая ходы по очереди, строят двуместную частичную функцию $F\colon X^2 \to X$. Игрок I определяет значения функции на множестве $\{(x, y) \in X^2 \mid x \in X_1\}$, а игрок II — на множестве $\{(x, y) \in X^2 \mid x \in X_2\}$. Своим ходом каждый игрок или определяет на своей области определения какое-либо значение функции F, или не делает ничего. Менять выбранные на предыдущих ходах значения нельзя. Игра выиграна игроком I, если после ω ходов формула Φ станет истинной на структуре $\langle X, F\rangle$; в противном случае игра выиграна игроком II.

Формула Φ называется *релятивизуемо истинной (ложной)*, если она истинна (ложна) на $\boldsymbol{A}$-вычислительных структурах при каждом оракуле $\boldsymbol{A}$. Нам будет удобно рассматривать функциональные оракулы, задаваемые всюду определённой функцией из $\mathbb{N}$ в $\mathbb{N}$. Оракул заданный функцией g можно отождествлять с оракулом, заданным характеристической функцией графика g.

Теорема II.4. *Замкнутая формула Φ в сигнатуре вычислительной структуры является релятивизуемо истинной тогда и только тогда, когда в игре $P(\Phi)$ у игрока* I *существует вычислимая выигрышная стратегия.*

Доказательство. Пусть формула Φ релятивизуемо истинна. Возьмём в качестве X натуральные, в качестве X_1 чётные и в качестве X_2 нечётные числа. Будем считать фиксированным вычислимое взаимно однозначное соответствие между множеством возможных ходов игроков и натуральным рядом. Стратегия для игрока I в игре $P(\Phi)$ состоит в том, что он вычислимым образом строит на своих номерах главную универсальную функцию H для одноместных функций, вычислимых относительно функции $g = \lambda n(n\text{-й ход игрока II})$. Функция $F(2k, y)$, построенная игроком I, вычисляет при фиксированном k функцию, имеющую номер k

в нумерации H. Так как функция $F\colon \mathbb{N}^2 \to \mathbb{N}$ вычислима относительно g и является главной нумерацией функций вычислимых относительно g, то формула Φ истинна в структуре $\langle \mathbb{N}, F\rangle$ (F — это построенная после ω ходов функция). Поэтому указанная для игрока I стратегия является выигрышной. Отметим, что эта стратегия не зависит от формулы Φ.

Пусть у игрока I существует вычислимая выигрышная стратегия. Фиксируем оракул $\boldsymbol{A}$. Предположим, игрок II строит на нечётных номерах какую-нибудь главную $\boldsymbol{A}$-нумерацию. Тогда построенная игроками функция F тоже является главной $\boldsymbol{A}$-нумерацией, и $\langle \mathbb{N}, F\rangle \models \Phi$. Поскольку все $\boldsymbol{A}$-вычислительные структуры изоморфны, формула Φ истинна в любой из этих структур. $\square$

Релятивизация этого доказательства даёт следующее.

Следствие II.4.1. *Пусть, $\boldsymbol{B}$ — какой-либо оракул. Замкнутая формула Φ произвольного языка в сигнатуре вычислительной структуры истинна для всех $\boldsymbol{A}$-вычислительных структур с $\boldsymbol{B} \leqslant \boldsymbol{A}$ тогда и только тогда, когда у игрока* I *существует в игре $P(\Phi)$ выигрышная стратегия, вычислимая относительно оракула $\boldsymbol{B}$.*

Следствие II.4.2. *Пусть, у игрока* I *существует в игре $P(\Phi)$ выигрышная стратегия. Тогда существует оракул $\boldsymbol{B}$ такой, что формула Φ истинна во всех $\boldsymbol{A}$-вычислительных структурах с $\boldsymbol{B} \leqslant \boldsymbol{A}$.*

Доказательство. В качестве оракула $\boldsymbol{B}$ можно взять выигрышную стратегию игрока I. $\square$

Теорема II.4 даёт схему доказательства релятивизуемой истинности некоторого свойства: нужно построить выигрышную стратегию для игрока I в соответствующей игре. Анализ обычных доказательств общей теории алгоритмов показывает, что почти все они легко укладываются в эту схему. Основную часть доказательства составляет описание конкретной стратегии и проверка того, что она выигрышная; вычислимость её устанавливается просто.

Игры Гейла—Стюарта

Описанная выше игра является частным случаем игр Гейла—Стюарта. Согласно Д. Мартину [**11**] игра Гейла—Стюарта определяется на дереве высоты ω с произвольным ветвлением. В ней участвуют два *игрока* I и II. *Игра* определяется разбиением множества всех путей, начинающихся из корня, на два множества: множество путей, выигрышных для игрока I, и множество путей, выигрышных для игрока II. *Позицией* игры является вершина дерева, *начальной* позицией является корень. *Ход* состоит в замене вершины на один из её непосредственных последователей. Игроки, делая ходы по очереди, строят некоторый путь. Выигрыш определяется принадлежностью построенного пути первому или второму множеству.

Стратегия игрока I (игрока II) — это функция, которая в каждой вершине чётной (нечётной) высоты указывает некоторый ход. Стратегия игрока I и стратегия игрока II вместе порождают некоторый путь. Если этот путь выигрышен для игрока I, скажем что стратегия игрока I *побеждает* стратегию игрока II. (Соответственно определим победу стратегии игрока II.) Назовём стратегию игрока *выигрышной*, если она побеждает все стратегии другого игрока. Игра называется *детерминированной*, если у одного из игроков есть выигрышная стратегия.

Введём на множестве всех путей, начинающихся из корня, каноническую топологию. Её базу составляют конуса, то есть множества всех путей, проходящих через как-либо фиксированную вершину. Отметим, что дополнение до конуса является открытым множеством.

Назовём игру *борелевской*, если выигрышные множества для игроков I и II являются борелевскими.

Теорема Мартина [**11**]. *Борелевские игры Гейла—Стюарта являются детерминированными.*

Игру $P(\Phi)$, заданную формулой Φ в сигнатуре вычислительной структуры, можно представить как игру Гейла—Стюарта $D(\Phi)$, которую мы сейчас опишем. Дерево этой игры в каждой вершине будет иметь счётное ветвление. Понятно, что вершину можно отождествлять с конечной последовательностью ходов, приводящих в эту вершину. Ходом может быть “пас” или элемент $\mathbb{N}^3$, интерпретируемый как точка графика функции двух аргументов из $\mathbb{N}$ в $\mathbb{N}$. При этом чётность первого аргумента должна быть равна чётности высоты вершины. Кроме того требуется, чтобы значение функции на той же паре аргументов не было определено на предыдущих шагах. Каждой вершине может быть сопоставлена функция из $\mathbb{N}^2$ в $\mathbb{N}$ с конечной областью определения, которая получается объединением ходов (не равных “пасу”), ведущих в эту вершину. Например, корню соответствует нигде не определённая функция. Каждому пути сопоставляется функция равная объединению ходов этого пути (кроме “пасов”). Путь объявляется выигрышным для игрока I, если соответствующая этому пути функция F удовлетворяет формуле Φ.

Добавим в язык $\mathrm{Th}\langle\mathbb{N}, F\rangle$ константы для всех натуральных чисел.

Теорема II.5. *Каждая замкнутая формула Φ языка $\mathrm{Th}\langle\mathbb{N}, F\rangle$, расширенного константами, задаёт борелевскую игру $D(\Phi)$.*

Доказательство. Будем рассуждать индукцией по построению формулы. Множество путей выигрышных для игрока I в игре $D(\exists x\,\Phi(x))$ является объединением всех множеств путей выигрышных для игрока I в играх $D(\Phi(n))$, $n \in \mathbb{N}$. Поэтому достаточно доказать, что замкнутая атомарная формула рассматриваемого языка задаёт борелевскую игру (в действительности, выигрышное множество оказывается даже открытым).

Истинность равенства двух замкнутых термов в данной интерпретации следует из истинности конъюнкции нескольких формул вида $F(k, m) = l$ в той же интерпретации. Указанная конъюнкция истинна для функции, сопоставленной некоторому пути, тогда и только тогда, когда она истинна для функции, сопоставленной одной из вершин этого пути. Последнее означает открытость выигрышного множества игрока I. $\square$

Получаются два важных следствия. Первое из них вытекает также из работы Д. Мартина [**12**].

Следствие II.5.1. *Для всякой замкнутой формулы Φ языка $\mathrm{Th}\langle\mathbb{N}, F\rangle$ либо Φ, либо отрицание Φ выполнено для всех $\boldsymbol{A}$-вычислительных структур при достаточно больших $\boldsymbol{A}$.*

Следствие II.5.2. *Существует такой оракул $\boldsymbol{B}$, что для всех оракулов $\boldsymbol{A} \geqslant \boldsymbol{B}$ все $\boldsymbol{A}$-вычислительные структуры элементарно эквивалентны.*

Доказательство. Для каждой замкнутой формулы Φ языка первого порядка рассмотрим оракул $\boldsymbol{C}_\Phi$ такой, что либо Φ, либо $\neg\Phi$ выполнено во всех $\boldsymbol{A}$-вычислительных структурах при $\boldsymbol{A} \geqslant \boldsymbol{C}_\Phi$. Оракул $\boldsymbol{B}$, равный прямой сумме всех оракулов $\boldsymbol{C}_\Phi$, обладает тем свойством, что у любой замкнутой формулы истинностное значение одинаково во всякой $\boldsymbol{A}$-вычислительной структуре при $\boldsymbol{A} \geqslant \boldsymbol{B}$. $\square$

Фактически, в обычных доказательствах общей теории алгоритмов рассматриваются игры, являющиеся той частью универсальной игры $D(\Phi)$, которая существенна для формулы Φ. Более точно, в частной игре множество позиций каждой высоты может быть получено факторизацией по разрешимому отношению эквивалентности множества позиций той же высоты в универсальной игре. Причём, предшественники эквивалентных позиций эквивалентны. Кроме того, если у двух бесконечных путей позиции равной высоты эквивалентны, то эти пути одновременно удовлетворяют или не удовлетворяют формуле Φ. Частная игра, в отличие от универсальной игры, бывает не симметричной. Её удобно неформально представлять себе как игру между Математиком и Природой. Математик стремится подтвердить выполненность Φ в математическом мире.

При этом Математик может произвольно устанавливать соотношения, но только на одной половине математического мира.

Представляется, что приведённый выше игровой подход интересно было бы обобщить в следующем направлении.

Игра типа $P(\Phi)$ может быть определена и на несчётных носителях. Это даёт возможность исследовать вычислимость на несчётных пространствах. Напомним, что теорема Мартина справедлива для борелевских ω-игр с любым ветвлением дерева игры.

ГЛАВА III

Об одной гипотезе А. Н. Колмогорова о случайных последовательностях

Будем рассматривать бесконечные двоичные последовательности как результаты последовательности независимых испытаний случайной величины со значениями 0, 1 и равномерным распределением вероятностей. Как определить случайность последовательности? Следующий способ был предложен А. Вальдом в 1938 году. Если фиксирован язык, то среди счётного класса определимых в нём множеств бесконечных двоичных последовательностей можно выделить те, которые имеют меру нуль. Случайными относительно фиксированного языка естественно называть последовательности, не лежащие ни в одном из выделенных множеств. Ясно, что почти все последовательности будут случайными. Этот подход связан с неопределённостью: какой язык выбрать?

Другой подход к определению случайности использует понятие энтропии конечной последовательности введённое А. Н. Колмогоровым. Заметим, что есть несколько определений энтропии; но их значения различаются не более чем на $O(\log n)$, где n — длина двоичной последовательности. Эта разница будет несущественной для наших результатов. Неформально говоря, бесконечная двоичная последовательность случайна, если энтропия её начал растёт достаточно быстро.

Мы исследуем также третий подход, сформулированный А. Н. Колмогоровым в 1963 году. Представим себе двусторонние карты. На лицевой стороне каждой из карт нарисована одна из цифр 0, 1. Оборотные стороны всех карт выглядят одинаково. Пусть дана последовательность карт, лежащих вверх оборотной стороной. Нас интересует, является ли случайной последовательность цифр, нарисованных на лицевых сторонах карт. Будем формировать вспомогательную двоичную последовательность, переворачивая карты в некотором порядке. Перед тем как перевернуть очередную карту будем решать, включить ли нарисованную на ней цифру во вспомогательную последовательность. Ко вспомогательной последовательности предъявляется *частотное требование*: доли нулей и единиц в началах последовательности должны стремиться к 1/2, когда длина начала стремится к бесконечности. Рассмотрим алгоритм, получающий на вход конечную последовательность цифр, нарисованных на уже перевёрнутых картах. На выход алгоритм даёт номер карты, которую следует перевернуть, и решение о включении нарисованной на ней цифры во вспомогательную последовательность. Каждый такой алгоритм порождает конечную или бесконечную *вспомогательную* последовательность.

Определение III.1. Бесконечная двоичная последовательность называется *стохастичной*, когда для всякой бесконечной вспомогательной последовательности выполнено частотное требование.

В 1968 году А. Н. Колмогоров предположил в [**2**], [**1**], что существует стохастичная последовательность, у которой энтропия начала длины n не превышает $O(\log n)$. Приведённая ниже теорема опровергает предположение Колмогорова.

Игры с переменными ставками

Сначала опишем класс конечных игр, которые будут использованы в основном доказательстве. В игре два участника — Математик и Казино. *Игра* задаётся двумя *параметрами*: натуральным числом m (продолжительность игры) и непустым множеством S двоичных последовательностей длины m. Оба параметра изначально известны обоим участникам. На нулевом шаге Казино выбирает во множестве S одну из последовательностей $\langle a_1, a_2, \ldots, a_m\rangle$. В продолжение игры эта последовательность не меняется. Математику выбор Казино неизвестен. Неформально говоря, на k-ом шаге ($1 \leqslant k \leqslant m$) Математик стремится угадать цифру a_k, используя информацию о цифрах с меньшими номерами. Теперь скажем формально: на k-ом шаге Математик указывает пару $\langle i(k), v(k)\rangle$, где $i(k)$ — двоичная цифра (предполагаемое значение a_k), а $v(k)$ — рациональное число из отрезка $[0, 1]$ (*ставка*). Для $0 \leqslant k \leqslant m$ определяется рациональное число V_k, называемое *капиталом*. Начальный капитал V_0 равен нулю. Если на k-ом шаге Математик не угадал цифру (то есть, если $i(k) \neq a_k$), то ставка теряется (то есть, $V_k = V_{k-1} - v(k)$). Если на k-ом шаге Математик угадал цифру, то $V_k = V_{k-1} + v(k)$. Цель Математика — достичь как можно большего капитала в конце игры. *Стратегией* назовём функцию, которая для всех положительных $k \leqslant m$ двоичным последовательностям длины $k-1$ сопоставляет пары $\langle i, v\rangle$, где i — цифра, а v — ставка. Если Казино выбрало последовательность $\langle a_1, a_2, \ldots, a_m\rangle$, то играя по стратегии σ, Математик указывает на k-ом шаге пару $\sigma(\langle a_1, \ldots, a_{k-1}\rangle)$.

Мощность множества S будем обозначать через $|S|$, логарифм по оснаванию два будем обозначать через lb.

Лемма III.1. *Для игры, заданной параметрами m и S, и рационального числа $r < m - \mathrm{lb}(|S|)$ существует стратегия σ, которая* *обеспечивает $V_m > r$ при любом выборе Казино. Эта стратегия эффективно находится по m, S и r.*

Доказательство. Немного изменим игру, сняв требование рациональности ставок. Построим стратегию с искомыми свойствами для изменённой игры. Нам понадобится следующее обозначение: если u — двоичная последовательность длины не более m, то S_u — это множество тех последовательностей из S, которые начинаются с u. Пусть, w — двоичная последовательность длины $k-1$ и $S_w \neq \varnothing$. Пусть, $|S_{w0}| \leqslant |S_{w1}|$ (противоположный случай рассматривается симметрично). Тогда стратегия сопоставляет последовательности w пару $\langle 1,\ 1-\mathrm{lb}(|S_w|)+\mathrm{lb}(|S_{w1}|)\rangle$. Видно, что ставка не больше единицы. Из $|S_{w0}| \leqslant |S_{w1}|$ следует $|S_{w1}| \geqslant |S_w|/2$, за счёт чего ставка неотрицательна.

Докажем, что как бы Казино не выбрало последовательность $\langle a_1, a_2, \ldots, a_m\rangle$ для всех $k \leqslant m$ будет

$$V_k \geqslant k + \mathrm{lb}\left(\left|S_{\langle a_1,\ldots,a_k\rangle}\right|\right) - \mathrm{lb}(|S|).$$

Для $k=0$ правая часть неравенства равна нулю. Затем рассуждаем индуктивно. Обозначим $\langle a_1,\ldots,a_{k-1}\rangle$ через w и предположим, что $|S_{w0}| \leqslant |S_{w1}|$. Рассмотрим два случая: $a_k = 1$ и $a_k = 0$. В первом случае доказываемое неравенство получается непосредственно. Во втором случае надо доказать, что

$$\begin{aligned}\big((k-1)+\mathrm{lb}(|S_w|)-\mathrm{lb}(|S|)\big) - \big(1-\mathrm{lb}(|S_w|)+\mathrm{lb}(|S_{w1}|)\big) \geqslant \\ \geqslant k+\mathrm{lb}(|S_{w0}|)-\mathrm{lb}(|S|).\end{aligned}$$

Это эквивалентно $2\,\mathrm{lb}(|S_w|) \geqslant 2+\mathrm{lb}(|S_{w1}|)+\mathrm{lb}(|S_{w0}|)$. Последнее неравенство получается после перехода к экспонентам с учётом того, что $|S_w| = |S_{w0}|+|S_{w1}|$.

Если Казино выбрало последовательность w, то $|S_w| = 1$ и $V_m \geqslant m - \mathrm{lb}(|S|)$. Приблизив ставки построенной стратегии рациональными числами, завершим доказательство леммы. □

Функцию энтропии будем обозначать через K. Начало длины n бесконечной последовательности A будем обозначать через $A \wr n$.

Теорема III.1. *Пусть D — вычислимая всюду определённая функция с натуральными аргументами и значениями. Если существует стохастичная последовательность A, у которой для всех достаточно больших n выполнено $K(A\wr n) < n - D(n)$, то при любом $\alpha > 0$ для всех достаточно больших n будет $D(n) < \alpha n$.*

Доказательство. Пусть D — вычислимая всюду определённая функция с натуральными аргументами и значениями; A — бесконечная двоичная последовательность, у которой для всех достаточно больших n выполнено $K(A \wr n) < n - D(n)$; α — положительное число и для бесконечно многих n имеет место $D(n) > \alpha n$. Наша цель предъявить алгоритм, выбирающий (не обязательно монотонно) из последовательности A бесконечную вспомогательную последовательность, которая не удовлетворяет частотному требованию.

Без ограничения общности можно считать, что $\alpha = M^{-1}$ и M — натуральное число. Длину конечной последовательности s будем обозначать через $\partial(s)$. Мы будем использовать следующее простое свойство энтропии: существует такая константа c, что для любых конечных последовательностей s, t выполнено $K(t) < K(st) + \partial(s) + c$. В дальнейшем через c будет обозначаться именно эта константа.

Свойства функции D позволяют фиксировать вычислимую возрастающую последовательность натуральных чисел, удовлетворяющую двум условиям:

(1) $D(n_k - 1) > \alpha(n_k - 1)$,

(2) $n_{k+1} > 200M^2(n_k + c)$.

Обозначим через N_k полуинтервал $[n_k, n_{k+1})$, а через $A \wr N_k$ последовательность $A(n_k), A(n_k+1), \ldots, A(n_{k+1}-1)$. Подставим в определении константы c вместо s и t последовательности $A \wr (n_k - 1)$ и $A \wr N_k$. Тогда получится

$$K(A \wr N_k) < K(A \wr n_{k+1} - 1) + n_k + c < (1-\alpha)n_{k+1} + n_k + c < \\ < (1 - \alpha/2)(n_{k+1} - n_k).$$

Как известно, функция энтропии перечислима сверху. То есть, существует вычислимый процесс, в котором появляются все истинные неравенства вида $K(t) < l$ и только они. Фиксируем один такой процесс. Обозначим через j_k время, за которое неравенство $K(A \wr N_k) < (1 - \alpha/2)(n_{k+1} - n_k)$ появляется в фиксированном процессе. Ключевое соображение: мы будем сравнивать значения j_k для разных k.

Нам предстоит построить $16M$ алгоритмов, один из которых выберет из последовательности A бесконечную вспомогательную последовательность, не удовлетворяющую частотному требованию. Половина этих алгоритмов будут называться *чётными*, и половина — *нечётными*. Нечётные алгоритмы переворачивают карты в монотонном порядке. Чётные алгоритмы переворачивают карты в следующем порядке. Сначала переворачиваются подряд карты с номерами из N_2, затем переворачиваются подряд карты с номерами из N_1; затем карты из N_4, затем карты из N_3; затем из N_6, затем из N_5 и так далее. Если для бесконечно многих k выполнено $j_{2k-1} \geqslant j_{2k}$, будут применяться нечётные алгоритмы. Если для бесконечно многих k выполнено $j_{2k-1} \leqslant j_{2k}$, будут применяться чётные алгоритмы. Один из двух указанных случаев имеет место. В силу симметрии достаточно рассмотреть случай чётных алгоритмов. Те k, для которых $j_{2k-1} \leqslant j_{2k}$, назовём *выгодными.*

Каждый чётный алгоритм задаётся парой *характеристик* $\langle d, z\rangle$, где d — двоичная цифра, а z — натуральное число между 1 и $4M$. Опишем действия алгоритма с характеристиками $\langle d, z\rangle$ для карт с номерами из N_{2k} и N_{2k-1}.

Алгоритм переворачивает все карты с номерами из N_{2k}, не включая нарисованные на них цифры во вспомогательную последовательность. Узнав последовательность $A \wr N_{2k}$, алгоритм ждёт пока истинное неравенство $K(A \wr N_{2k}) < (1-\alpha/2)(n_{2k+1} - n_{2k})$ появится в процессе перечисления. Тем самым станет известным число j_{2k}. Найдём множество S двоичных последовательностей u длины $m = n_{2k} - n_{2k-1}$, для которых неравенство $K(u) < (1-\alpha/2)(n_{2k} - n_{2k-1})$ появляется в процессе перечисления за время не большее j_{2k}. При выгодных k, последовательность $A \wr N_{2k-1}$ попадает во множество S. Рассмотрим стратегию σ, построенную в лемме III.1 для игры с параметрами m и S. Как известно, мощность множества тех u, для которых $K(u) < l$, меньше 2^{l+1}. Поэтому $|S| < 2^{(1-\alpha/3)m}$. По лемме III.1 при выгодных k стратегия σ приводит к заключительному капиталу $V_m > \alpha m/3$. Переделаем стратегию σ в следующую стратегию δ с теми же параметрами. Когда по стратегии σ Математик указывал пару $\langle i, v\rangle$, по стратегии δ Математик укажет пару $\langle i,\ \lfloor 4Mv\rfloor/4M\rangle$. Изменение заключительного капитала стратегии δ по сравнению с заключительным капиталом стратегии σ меньше $\alpha m/4$. Так что при выгодных k заключительный капитал стратегии δ будет больше $\alpha m/12$. Алгоритм включает карту с номером из N_{2k-1} во вспомогательную последовательность, если стратегия δ указывает пару $\langle d, \alpha z/4\rangle$.

Теперь докажем, что один из построенных чётных алгоритмов сформирует вспомогательную последовательность, не удовлетворяющую частотному требованию. Для этого каждой паре характеристик $\langle d, z\rangle$ сопоставим в игре с параметрами m и S стратегию $\delta_{d,z}$. Когда по стратегии δ Математик указывал пару $\langle d, z/4M\rangle$, по стратегии $\delta_{d,z}$ Математик укажет ту же пару. В остальных случаях Математик сделает нулевую ставку. Понятно, что заключительный капитал стратегии δ равен сумме заключительных капиталов стратегий $\delta_{d,z}$. Следовательно при выгодных k для одной из пар $\langle d, z\rangle$ заключительный капитал стратегии $\delta_{d,z}$ будет больше $\alpha^2 m/96$. Скажем, что число k *соответствует* такой паре характеристик $\langle d, z\rangle$. Рассмотрим разность между количествами цифр d и $(1-d)$, включённых алгоритмом с характеристиками $\langle d, z\rangle$ во вспомогательную последовательность при переворачивании карт с номерами из N_{2k-1}. Поскольку ставки не превышают единицы, эта разность не меньше заключительного капитала стратегии $\delta_{d,z}$. (Напомним, что в стратегии $\delta_{d,z}$ все ненулевые ставки одинаковы.) Количество цифр, включённых во вспомогательную последовательность при переворачивании карт с номерами меньшими n_{2k-1}, не превышает n_{2k-1}. Поэтому разность H между количествами цифр d и $(1-d)$, включённых алгоритмом во вспомогательную последовательность при переворачивании карт с номерами меньшими n_{2k}, оказывается больше $\alpha^2(n_{2k}-n_{2k-1})/96-n_{2k-1}$. За счёт условия (2) последнее число больше $\alpha^2 n_{2k}/200$. Отношение числа H к количеству цифр, включённых во вспомогательную последовательность при переворачивании карт с номерами меньшими n_{2k}, получается больше $\alpha^2/200$. Остаётся заметить, что бесконечно много выгодных чисел k соответствуют одной паре характеристик. □

В заключение, поставим открытую проблему.

Сохранится ли правильность теоремы III.1, если в её формулировке не использовать условие вычислимости функции D?

Литература

[1] Колмогоров А.Н. *К логическим основам теории информации и теории вероятностей.* Проблемы передачи информации, т. 5, вып. 3 (1969) 3–7.

[2] Колмогоров А.Н. *Logical basis for information theory and probability theory.* IEEE Trans. Inform. Theory IT-14 (1968) 662–664.

[3] Мучник Ан.А. *Игры на бесконечных деревьях и автоматы с тупиками. Новое доказательство разрешимости монадической теории двух следований.* Семиотика и информатика, вып. 24 (1985) 16–40.

[4] Мучник Ан.А. *Об основных структурах дескриптивной теории алгоритмов.* Доклады Академии Наук СССР, т. 285, № 2 (1985) 280–283.

[5] Мучник Ан.А., Семёнов А.Л., Успенский В.А. *Mathematical metaphysics of randomness.* Theoretical Computer Science, v. 207 (1998) 263–317.

[6] Мучник Ан.А. *Games on infinite trees and automata with dead-ends. A new proof for the decidability of the monadic second order theory of two successors.* Bulletin of the European Association for Theoretical Computer Science, v. 48 (1992) 219–267.

[7] Селиванов В.Л. *A logical approach to decidability of hierarchies of regular star-free languages.* 18-th International Symposium on Theoretical Aspects of Computer Science, Germany (2001).

[8] Успенский В.А., Семёнов А.Л. *Теория алгоритмов: основные открытия и приложения.* Москва «Наука» (1987).

[9] Büchi J.R. *On a decision method in restricted second order arithmetic.* Proceedings of the international congress of Logic, Methodology and Philosophy of Science; Stanford (1962) 1–11.

[10] Friedman H. *Axiomatic recursive function theory.* Logic Colloquium 1969, North-Holland (1971) 113–137.

[11] Martin D.A. *Borel determinacy.* Annals of Mathematics, v. 102 (1975) 363–371.

[12] Martin D.A. *The axiom of determinateness and reduction principles in the analytical hierarchy.* Bulletin of AMS, v. 74 (1968) 687–689.

[13] McNaughton R. *Testing and generating infinite sequences by finite automata.* Information and Control, v. 9, n. 5 (1966) 521–530.

[14] Rabin M.O. *Decidability of second order theories and automata on infinite trees.* Transactions of AMS, v. 141 (1969) 1–35.

[15] Rabin M.O. *Decidability and definability in second order theories.* Actes du Congr. Int. des Math., Nica, v. 1 (1970) 239–244.

[16] Rogers H.(Jr) *Gödel numberings of partial recursive functions.* Journal of Symbolic Logic, v. 23, n. 3 (1958) 331–341.

[17] Siefkes D. *Büchi's monadic second order successor arithmetic.* Lecture Notes in Mathematics, v. 120 (1970).

Оглавление

Предисловие 2

Глава I. Упрощённое доказательство теоремы Рабина о разрешимости монадической теории дерева 6

§ 1. Монадическая теория двух следований и конечные автоматы на деревьях 7

Автоматы на сверхсловах 8

Автоматы на деревьях 10

§ 2. Доказательство теоремы об автоматности дополнения 11

Стратегии 11

Модификация понятия стратегии — стратегии с памятью 13

Введение тупиков в автоматы и стратегии 15

Случай автомата с одним состоянием 17

Шаг индукции (описание стратегического множества и соответствующие леммы) 20

Завершение шага индукции 23

Завершение доказательства теоремы о дополнении 25

§ 3. Об аксиоматизации $S2S$ 27

Глава II. Характеризация релятивизуемых утверждений общей теории алгоритмов в игровых терминах 29

Вычислительная структура 29

Релятивизованные вычислительные структуры 31

Пример нерелятивизуемой формулы 33

Игровая интерпретация 34

Игры Гейла—Стюарта 35

Глава III. Об одной гипотезе А. Н. Колмогорова о случайных последовательностях 39

Игры с переменными ставками 40

Литература 45