Ученые записки

ТЕОРИЯ АЛГОРИТМОВ И ПРОГРАММ

II

Министерство высшего и среднего специального
образования Латвийской ССР

Латвийский ордена Трудового Красного Знамени
государственный университет имени Петра Стучки

Вычислительный центр

Ученые записи
Латвийского государственного университета
имени Петра Стучки

том 233

ТЕОРИЯ АЛГОРИТМОВ И ПРОГРАММ

Выпуск II

Латвийский государственный университет

Рига 1975

УДК 51.01:513.5

Сборник "Теория алгоритмов и программ, II" посвящен в основном теории индуктивного вывода. Рассматриваются также вопросы проверки правильности гипотез (в более практическом плане), связанные с отладкой программ. Отдельные статьи излагают результаты по близким вопросам теории автоматов (автоматы Бухбергера, вычисления в реальное время и др.).

Сборник рассчитан на научных работников, занимающихся или интересующихся теорией алгоритмов и программ, на аспирантов и студентов.

Т $\frac{20205-152\text{у}}{\text{М } 812(\text{II})-75}$ 144-75

ВОЗМОЖНОСТИ ПРЕДЕЛЬНОГО СИНТЕЗА НОМЕРОВ ОБЩЕРЕКУРСИВНЫХ ФУНКЦИЙ В РАЗЛИЧНЫХ ВЫЧИСЛИМЫХ НУМЕРАЦИЯХ

Р.В.Фрейвалд

В [I-4] изучалась задача предельного синтеза номера общерекурсивной (сокращенно: о.р.) функции по значениям этой функции при различных значениях аргумента. Рассмотрим необходимые определения.

Пусть зафиксированы некоторая нумерация ν всех одноместных частично рекурсивных (ч.р.) функций и некоторая канторовская (т.е. вычислимая взаимно однозначная) нумерация $\langle x_1, \dots, x_n \rangle$ всевозможных кортежей $\{x_1, \dots, x_n\}$ (произвольной длины) натуральных чисел. Стратегией называется произвольная ч.р. функция F. Говорят, что стратегия F предельно синтезирует ν-номер о.р. функции f, если I) для любого натурального n определено значение $F(\langle f(0), f(1), \dots, f(n) \rangle)$, и 2) предел $\lim\limits_{n\to\infty} F(\langle f(0), f(1), \dots, f(n) \rangle)$ существует и равен некоторому номеру функции f в нумерации ν. Говорят, что класс U о.р. функций предельно ν-синтезируем, если существует стратегия F, которая предельно синтезирует ν-номера всех функций класса U.

В [I-4] рассматривался предельный синтез номеров в главных вычислимых нумерациях φ (определение см., например, [5]) всех одноместных ч.р. функций. В настоящей работе изучается предельная ν-синтезируемость классов о.р. функций при различных вычислимых нумерациях ν всех одноместных ч.р. функций.

Так как любая вычислимая нумерация ν сводится к любой главной вычислимой нумерации φ, то из предельной ν-синтезируемости любого класса U следует также предельная φ-синтезируемость. Когда выяснилось, что существует такая вычислимая нумерация ν, что не всякий предельно φ-синтезируемый класс является также предельно ν-синтезируемым, Я.М.Барздинь поставил вопрос о характеризации тех классов, которые предельно ν-синтезируемы при всех вычислимых нумерациях ν всех ч.р. функций. Теорема I и ее следствие дают ответ на этот вопрос. Далее предпринята попытка хотя бы частично выяснить, что делает вычислимую нумерацию "плохой" для предельного синтеза. Показано, что ограниченность числа различных номеров одной и той же о.р. функции является фактором такого рода.

ТЕОРЕМА I. Существует такая вычислимая нумерация ν всех одноместных ч.р. функций, что никакой бесконечный класс о.р. функций не является предельно ν-синтезируемым.

Прежде чем приступить к доказательству теоремы, докажем ряд лемм и определим требуемую нумерацию ν. Введем и ряд обозначений, которые понадобятся также для доказательства дальнейших теорем.

Через ν_n и φ_n будем обозначать (соответственно) функции с номером n в нумерациях ν и φ. Канторовскую нумерацию пар натуральных чисел будем задавать функциями c, ℓ, r $(c(x,y)=u,\ \ell(u)=x,\ r(u)=y)$.
В доказательстве теоремы 2 будут использованы более тонкие свойства функций c, ℓ, r. Поэтому с самого начала будем считать, что эта нумерация распологает пары в следующем порядке:

(0,0); (0,I), (I,0); (0,2),(I,I),(2,0); (0,3),(I,2),...

ЛЕММА I.I. Существует такая всюду определенная функция f с графиком, принадлежащим Π_1, что I) для любой ч.р. функции ψ равенства $\psi(x)=f(x)$ могут быть истинны лишь для конечного числа различных x, 2) $\forall x\ \exists p\ (f(x)=c(x,p))$.

ДОКАЗАТЕЛЬСТВО. Для доказательства принадлежности графика функции f классу Π_1 иерархии Клини-Мостовского нужно показать, что существует алгоритм $\mathfrak{A}$, который по данным x,y при $f(x)\neq y$ останавливается и выдает результат I, при $f(x)=y$ не останавливается.

Сначала мы опишем вспомогательный алгоритм $\mathfrak{B}$, который, имея только один аргумент x, выдает бесконечную последовательность всевозможных истинных неравенств $f(x)\neq u$, содержащих данное x. Так как $\mathfrak{B}$ будет обладать свойством на каждом x выдавать неравенства $f(x)\neq u$ для всевозможных натуральных u, кроме одного, то алгоритм $\mathfrak{B}$ задаст функцию f, определенную однозначно.

Алгоритм $\mathfrak{B}$ работает следующим образом. Параллельно вычисляются $\varphi_0(x), \varphi_1(x), \dots, \varphi_x(x)$ в течение I,2, 3, ... тактов работы машины Тьюринга. Параллельно с этим одно за другим выдаются неравенства $f(x)\neq 0, f(x)\neq 1, f(x)\neq 2, \dots$ $\dots, f(x)\neq c(x,0)-1,\ f(x)\neq c(x,0)+1,\ f(x)\neq c(x,0)+2, \dots$

Если останавливается вычисление какого-то $\varphi_{i_0}(x)$ из $\varphi_0(x), \varphi_1(x), \dots, \varphi_x(x)$, то $\mathfrak{B}$ сравнивает, не совпадает ли $\varphi_{i_0}(x)$ с $c(x,0)$. Если не совпадает, то продолжает выдаваться начатая последовательность неравенств. Если совпадает, то $\mathfrak{B}$ выдает неравенство $f(x)\neq c(x,0)$, находит минимальное такое p_1, что неравенство $f(x)\neq c(x,p_1)$ еще не выдано, и в дальнейшем выдает неравенства

$$\dots, f(x)\neq c(x,p_1)-2, f(x)\neq c(x,p_1)-1,\ f(x)\neq c(x,p_1)+1, f(x)\neq c(x,p_1)+2, \dots$$

Параллельно продолжается вычисление остальных $\varphi_0(x), \varphi_1(x), \ldots, \varphi_x(x)$. В случае остановки еще одного из этих вычислений аналогично проверяется, совпадают ли $\varphi_{i_1}(x)$ и $c(x,p_1)$ и т.д.

Список $\varphi_0(x), \varphi_1(x), \ldots, \varphi_x(x)$ имеет конечную длину, поэтому таких сравнений будет только конечное число и $f(x)$ окажется определенной. Легко видеть, что f^* удовлетворяет и всем другим требованиям леммы. Перестроить алгоритм $\mathscr{L}$ в требуемый алгоритм $\mathfrak{A}$ также не представляет труда.

Незначительно усложнив это доказательство, можно доказать следующую лемму.

ЛЕММА I.2. Существует такая всюду определенная функция f с графиком, принадлежащим Π_2, что I) для любой (частичной) функции ψ с графиком, принадлежащим Σ_2, равенства $\psi(x)=f(x)$ могут быть истинны лишь для конечного числа различных x, 2) $\forall x \exists p (f(x)=c(x,p))$.

Доказательство опустим, отметив только, что принадлежность графика функции f классу Π_2 можно представить как наличие алгоритма $\mathfrak{A}$, который по любым данным x, y выдает бесконечную последовательность нулей и единиц, причем, если $f(x)=y$, то последовательность содержит бесконечно много единиц, и если $f(x)\neq y$, то - только конечное число.

Используем теперь алгоритм $\mathfrak{A}$ для функции f из леммы I.2 для определения нужной нам нумерации ν. Фридберг [6] доказал существование вычислимой однозначной нумерации ν' всех ч.р. функций (нумерация ч.р. функций называется однозначной, если каждая ч.р. функция имеет в ней ровно один номер). Функция $\nu_n(t)$ определяется так: она принимает значение $\nu'_{\ell(n)}(t)$, если $\mathfrak{A}$ по данным $x=\ell(n)$, $y=r(n)$ выдает последовательность содержащую не менее t единиц, и не определена в противном случае.

ЛЕММА I.3. ν является вычислимой нумерацией всех ч.р. функций, в которой каждая о.р. функция имеет ровно один номер.

ДОКАЗАТЕЛЬСТВО. Если некоторая функция ψ имеет в нумерации ν' номер n, то $c(n,f(n))$ является ее номером в нумерации ν, а все числа вида $c(n,p)$ (где $p \neq f(n)$) являются номерами функций, определенных только в конечном числе точек. Следовательно, если ψ имеет бесконечную область определения, то в нумерации ν она не имеет номеров, отличных от $c(n,f(n))$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ I. Допустим от противного, что бесконечный класс о.р. функций предельно ν -синтезируем стратегией F.

Определим вспомогательную функцию $\eta(x,t)$:

$$\eta(x,t) = \begin{cases} 0, & \text{если } t=0 \\ F(\langle \nu'_x(0), \nu'_x(1), \ldots, \nu'_x(t-1)\rangle), & \text{если } t>0 \end{cases}$$

К сожалению, функция $\eta(x,t)$ является только частично рекурсивной. Определим другую вспомогательную функцию, которая является общерекурсивной: для вычисления $g(x,t)$ нужно вычислять последовательно значения $\eta(x,0)$, $\eta(x,1)$, $\eta(x,2), \ldots$, затратив t тактов суммарного машинного времени. Тогда $g(x,t)$ равно последнему полностью вычисленному за это время члену указанной последовательности (и равно 0, если t тактов недостаточно для вычисления $\eta(x,0)$). Определим $\psi(x)$ как $\lim_{t\to\infty} r(g(x,t))$. Так как ψ является пределом о.р. функции, по [7] график ψ принадлежит Σ_2 .

Вспомним, что каждая о.р. функция имеет в нумерациях ν' и ν по одному номеру, и если номер какой-то о.р. функции в нумерации ν' равен n , то в нумерации

ν ее номер равен $c(n,f(n))$. Если стратегия F предельно синтезирует ν -номер функции ν_n', то $\lim\limits_{t\to\infty} \eta(n,t) = c(n,f(n))$. Следовательно, $\lim\limits_{t\to\infty} g(n,t)$ также равен $c(n,f(n))$ и $\psi(n) = \lim\limits_{t\to\infty} r(g(n,t)) = f(n)$. Но по лемме I.2. значения функций ψ и f могут совпадать только в конечном числе точек. Теорема доказана.

Так как любой класс всюду определенных функций, состоящий только из конечного числа функций, предельно ν -синтезируем при любой (не обязательно даже вычислимой) нумерации ν, получается следующее решение вопроса Я.М.Барздиня.

СЛЕДСТВИЕ. Класс U о.р. функций предельно ν -синтезируем при всех вычислимых нумерациях ν всех ч.р. функций тогда и только тогда, когда U состоит из конечного числа функций.

ЗАМЕЧАНИЕ I. Обозначим, как обычно, сводимость нумерации ν' к нумерации ν'' через $\nu' \leqslant \nu''$. Пусть $\mathcal{L}_1$ - частичный порядок классов эквивалентностей относительно сводимости всех вычислимых нумераций всех одноместных ч.р. функций. Обозначим через $\nu' \leqslant_{synt} \nu''$ следующее свойство пары нумераций: для любого класса U о.р. функций из предельной ν' -синтезируемости U вытекает предельная ν'' -синтезируемость класса U.
Пусть $\mathcal{L}_2$ -частичный порядок классов эквивалентностей всех вычислимых нумераций всех одноместных ч.р. функций относительно $\leqslant_{synt}$. Из $\nu' \leqslant \nu''$ вытекает $\nu' \leqslant_{synt} \nu''$.

Теорема I и ее следствие показывают, что в $\mathcal{L}_2$ существует наименьший элемент. В то же время наименьшего элемента в $\mathcal{L}_1$ не существует. Следовательно, $\mathcal{L}_2$ отличается от $\mathcal{L}_1$, и существуют такие нумерации ν' и ν'', что $\nu' \leqslant_{synt} \nu''$, но $\nu' \nleqslant \nu''$.

Вместо обычной сводимости в этом замечании можно было рассматривать "предельную сводимость" и получить аналогичное заключение.

ЗАМЕЧАНИЕ 2. Известно (см. [5]), что $\mathcal{C}_1$ не является нижней полурешеткой. Можно убедиться, что $\mathcal{C}_2$ является таковой. Более того, $\mathcal{C}_2$ -дистрибутивная решетка. Действительно, в качестве точной нижней грани классов, содержащих нумерации ν' и ν'' , можно рассматривать класс, содержащий нумерацию $\nu' \otimes \nu''$, которая определяется следующим образом:

$$(\nu' \otimes \nu'')_{c(i,j)}(x) = \begin{cases} \nu'_i(x) & \text{, если } \nu'_i(x) = \nu''_j(x) \\ \text{не определено, в противном случае} \end{cases}$$

В этом замечании существенно используется то, что мы интересуемся предельным синтезом только о.р. функций.

Класс о.р. функций называется эффективно перечислимым, если он имеет вычислимую нумерацию (другими словами, если он имеет о.р. универсальную функцию). Э.М.Голд [8] показал, любой эффективно перечислимый класс предельно φ -синтезируем при любой главной вычислимой нумерации φ всех ч.р.функций. Поэтому эффективно перечислимые классы можно рассматривать как "простейшие" предельно φ - синтезируемые классы.

Следующие две теоремы, однако, показывают, что для неглавных вычислимых нумераций ν свойство допускать бесконечные предельно ν-синтезируемые эффективно перечислимые классы и свойство допускать другие бесконечные предельно ν - синтезируемые классы о.р. функций в каком-то смысле независимы.

ТЕОРЕМА 2. Существует такая вычислимая нумерация ν всех ч.р. функций, что I) существует бесконечный предельно ν -синтезируемый класс о.р. функций, и 2) никакой бесконечный эффективно перечислимый класс не является предельно ν - синтезируемым.

Перед доказательством теоремы рассмотрим две леммы. Известно, что теорему Поста о существовании простого множества можно несколько усилить(см. [9]).

ЛЕММА 2.1. Существует такое множество A , что 1) A рекурсивно перечислимо, 2) для любого m среди чисел $0, 1, 2, \ldots, m$ имеется не более $\log_2 m$ элементов множества A , 3) $\bar{A}$ не имеет бесконечных рекурсивно перечислимых подмножеств.

ДОКАЗАТЕЛЬСТВО. Пусть W_x -область определения функции φ_x , $B = \{\langle x, y \rangle | \ y \in W_x \ \& \ y \geqslant 2^{x+1}\}$. Фиксируем некоторый эффективный пересчет множества B . Образуем множество $B' = \{\langle x, y \rangle | \quad \langle x, y \rangle \in B \ \&$

$\& (\forall z) [[z \neq y \ \& \ \langle x, z \rangle \in B] \Rightarrow \langle x, z \rangle$ идет позже $\langle x, y \rangle$ в этом пересчете $B]\}$. Определяем $A = \{ y | (\exists x) [\langle x, y \rangle \in B'] \}$. Свойства 1), 3) доказывают таким же образом, как в теореме Поста (см. например, [10]). Свойство 2) следует из $y \geqslant 2^{x+1}$ в определении множества B .

Применением релятивизации с креативным оракулом из доказательства леммы 2.1. можно получить доказательство следующей леммы.

ЛЕММА 2.2. Существует такое множество A что 1) $A \in \Sigma_2$ 2) для любого m среди чисел $0, 1, 2, \ldots, m$ имеется не более $\log_2 m$ элементов множества A , 3) $\bar{A}$ не имеет бесконечных подмножеств, принадлежащих классу Σ_2.

Теперь мы в состоянии доказать теорему 2.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2.

1. Пусть φ - главная вычислимая нумерация всех ч.р. функций. Рассмотрим две вспомогательные нумерации всех ч.р. функций:

$$\varphi'_i(x) = \begin{cases} \varphi_j(x) & \text{, если } i = 2j \\ j & \text{, если } i = 2j+1, \end{cases}$$

$$\varphi''_i(x) = \varphi'_{\ell(i)}(x).$$

В силу выбора конкретных канторовских нумерационных функций c, ℓ, r для нумерации φ'' выполняется следующее важное свойство: для любых n, k среди функций φ''_0, $\varphi''_1, \varphi''_2, \dots, \varphi''_{k^2}$ не менее чем $k-n$ раз встречается функция φ'_n.

2. Определим нумерацию ν, пользуясь нумерацией φ'' и множеством A из леммы 2.2. $A \in \Sigma_2$, следовательно, частично характеристическую функцию множества A

$$\chi_A(y) = \begin{cases} 1 & \text{, если } y \in A \\ \text{не опр., если } & y \in \bar{A} \end{cases}$$

можно представить в виде предела подходящей о.р. функции: $\chi_A(y) = \lim_{s \to \infty} h(y, s)$. Для любых i, x значение функции $\nu_i(x)$ тогда определяется так: если в последовательности значений $h(i,0), h(i,1), h(i,2), \dots$ имеется не менее x значений, отличных от 1, то $\nu_i(x) = \varphi''_i(x)$; иначе $\nu_i(x)$ не определена. Легко видеть, что если i является φ''-номером функции с бесконечной областью определения, то $(\nu_i = \varphi''_i) \Longleftrightarrow (i \in \bar{A})$.

3. Докажем, что ν -нумерация всех ч.р. функций. Действительно, по свойству нумерации φ'', для любых n, k среди функций $\varphi''_0, \varphi''_1, \varphi''_2, \dots, \varphi''_{k^2}$ не менее чем $k-n$ раз встречается функция φ'_n. Для любого n существует такое k, что $k-n$ больше, чем $(1+\log_2 k^2)$. Поэтому для этого k существует такое $i \in \{0, 1, 2, \dots, k^2\}$, что $i \in \bar{A}$ и одновременно i является номером функции φ'_n в нумерации φ''. Но тогда i является также номером φ'_n в нумерации ν.

4. Докажем теперь, что никакой бесконечный эффективно перечислимый класс не является предельно ν -синтезируемым.

Пусть некоторая стратегия F предельно ν -синтезирует некоторый эффективно перечислимый класс $U = \{\alpha_i(x)\}$.

Пусть

$$g(i,n) \underset{def}{=} F(\langle \alpha_i(0), \alpha_i(1), \dots, \alpha_i(n) \rangle)$$

и пусть $\psi(i) \underset{def}{=} \lim_{n\to\infty} g(i,n)$. Функция $\psi(i)$ определена как предел о.р. функции. Следовательно, область ее значений принадлежит Σ_2 . Так как F синтезирует класс U правильно, и все функции этого класса общерекурсивны, то $\{\psi(0), \psi(1), \psi(2), \dots\} \subseteq \bar{A}$ и, если α_i и α_j - различные функции, то $\psi(i) \neq \psi(j)$. Тогда по утверждению 3) леммы 2.2. область значений функции ψ конечна, и, следовательно, U содержит только конечное число различных функций.

5. Докажем, что бесконечный предельно ν -синтезируемый класс о.р. функций тем не менее существует.

Рассмотрим эффективно перечислимый класс U_0 , состоящий из всех константных функций. Определим стратегию $G(\langle y_0, y_1, \dots, y_n \rangle) = c(2\cdot y_0 + 1, 0)$. Стратегия G правильно синтезирует φ'' -номера всех функция класса U_0 Воспользуемся теперь свойством нумерации ν , отмеченным в п.2: если i является φ''-номером о.р. функции, то $(\nu_i = \varphi_i'') \Longleftrightarrow (i \in \bar{A})$.

Обозначим множество

$$\{c(2\cdot 0+1,0),\ c(2\cdot 1+1,0),\ c(2\cdot 2+1,0),\ \dots\}$$

через C . Из свойства функций c, ℓ, r вытекает, что для любого κ пересечение C с множеством $\{0,1,2,\dots,2\kappa^2+\kappa\}$ содержит не менее чем κ элементов. С другой стороны, множество $\{0,1,2,\dots,2\kappa^2+\kappa\}$ может содержать не более $\log_2(2\kappa^2+\kappa)$ элементов множества A . Поэтому $C \cap \bar{A}$ бесконечно. Следовательно, стратегия G предельно ν -синтезирует бесконечный подкласс класса U_0 . Теорема доказана.

ТЕОРЕМА 3. Существует такая вычислимая нумерация ν всех ч.р. функций, что I) существует бесконечный эффективно перечислимый предельно ν -синтезируемый класс,

2) любой предельно ν - синтезируемый класс о.р. функций содержится в предельно ν -синтезируемом эффективно перечислимом классе.

ДОКАЗАТЕЛЬСТВО. Пусть ν^0 -нумерация, существование которой утверждает теорема I. Рассмотрим нумерацию ν , для которой

$$\nu_i(x) = \begin{cases} \nu^0_j(x) & \text{, если } i = 2j \\ j & \text{, если } i = 2j+1 \end{cases}$$

Бесконечный эффективно перечислимый класс U_0 всех константных функций предельно ν -синтезируем стратегией $G(\langle y_0, y_1, \dots, y_n \rangle) = 2y_0 + 1$.

Докажем утверждение 2). Пусть U -произвольный предельно ν -синтезируемый класс. $U \setminus U_0$ не может быть бесконечным, так как это противоречило бы теореме I - ведь класс $U \setminus U_0$ предельно ν -синтезируем тогда и только тогда, когда он предельно ν^0 -синтезируем. Поэтому $U \setminus U_0$- конечный или пустой класс, и U содержится в эффективно перечислимом предельно ν -синтезируемом классе $U_0 \cup (U \setminus U_0)$.
Теорема доказана.

Следующая теорема и, даже в большей мере, ее следствие призваны дать хотя бы частичный ответ на вопрос, какие факторы делают вычислимую нумерацию "плохой" для предельного синтеза. Эта теорема возникла как обобщение одного результата Е.Б.Кинбера [II] . Им была доказана теорема, из которой вытекает, что для любой главной вычислимой нумерации φ всех одноместных ч.р. функций существует эффективно перечислимый класс, для которого нельзя предельно синтезировать минимальные φ -номера. Ниже будет показано, что в этом следствии существенно не то, что номера являются минимальными, а то, что из бесконечного множества всех номеров данной функции нужно выбрать заранее фиксированный номер.

Пусть ν -произвольная нумерация всех ч.р.функций и c -произвольное натуральное число. Будем называть фиксацией ν-номеров любое отображение μ , сопоставляющее каждой о.р. функции f некоторое непустое множество $\mu(f)$ номеров функции f в нумерации ν . Будем говорить, что фиксация ν -номеров является c -ограниченной, если для каждой о.р.функции f множество $\mu(f)$ состоит из не более чем c элементов. Будем говорить, что класс U о.р.функций предельно μ-ν -синтезируем, если существует ч.р.стратегия, которая по каждой функции $f \in U$ предельно синтезирует некоторый номер из $\mu(f)$.

ТЕОРЕМА 4. Пусть ν - произвольная вычислимая нумерация всех ч.р.функций и пусть c -произвольное натуральное число. Тогда для любой c -ограниченной фиксации ν -номеров μ существует эффективно перечислимый класс о.р. функций, который не является предельно μ-ν -синтезируемым.

ЛЕММА 4.1. Для любой главной вычислимой нумерации φ всех ч.р.функций существует такая о.р.функция g ,что: 1) при любом i функция $\varphi_{g(i)}$ общерекурсивна, 2) для любой нумерации ν всех ч.р. функций, для каждой фиксации μ ν -номеров и для любого класса U о.р. функций, если φ_i предельно μ-ν -синтезирует класс U то $\varphi_{g(i)}$ также предельно μ-ν -синтезирует класс U .

ДОКАЗАТЕЛЬСТВО. Для вычисления $\varphi_{g(i)}(\langle y_0, y_1, \ldots, y_n\rangle)$ вычисляем $\varphi_i(\langle y_0\rangle)$, $\varphi_i(\langle y_0, y_1\rangle), \ldots, \varphi_i(\langle y_0, y_1, \ldots y_n\rangle)$, каждое в течение $n+1$ тактов работы машины Тьюринга. Если вычисление $\varphi_i(\langle y_0\rangle)$ за это время не остановилось, то $\varphi_{g(i)}(\langle y_0, y_1, \ldots, y_n\rangle) = 0$. В противном случае находим наибольшее такое $t \leq n$, что вычисление каждого из $\varphi_i(\langle y_0\rangle)$, $\varphi_i(\langle y_0, y_1\rangle), \ldots, \varphi_i(\langle y_0, y_1, \ldots, y_t\rangle)$ останавливается за $n+1$ тактов, и определяем $\varphi_{g(i)}(\langle y_0, y_1, \ldots, y_n\rangle)$

равным $\varphi_i(\langle y_0, y_1, \ldots, y_t\rangle)$. Легко видеть, что если для какой-то последовательности $y_0, y_1, y_2, \ldots$ существует предел $\lim\limits_{n\to\infty} \varphi_i(\langle y_0, y_1, \ldots, y_n\rangle)$, то существует и предел $\lim\limits_{n\to\infty} \varphi_{g(i)}(\langle y_0, y_1, \ldots, y_n\rangle)$ и эти пределы равны.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 4. Пусть μ -произвольная фиксация ν -номеров о.р.функций. Пусть нумерация ν и фиксация μ таковы, что для любого эффективно перечислимого класса существует ч.р. стратегия F, которая предельно $\mu-\nu$ -синтезирует этот класс. Из леммы 4.I. вытекает, что без ущерба для общности стратегию F можно полагать общерекурсивной.

В процессе доказательства будут построены такие эффективно перечислимые классы $U_1, U_2, U_3, \ldots$, что для любого натурального c предельная $\mu-\nu$ -синтезируемость одновременно всех классов $U_1, U_2, \ldots, U_{c+1}$ не совместима с c -ограниченностью фиксации μ. Построение указанных классов будет проводиться индукцией по номеру класса.

<u>Базис индукции</u>. U_1 определяется как класс, состоящий из всевозможных о.р.функций f, для которых $\lim\limits_{x\to\infty} f(x)=0$. Класс U_1 эффективно перечислим, поэтому по допущению существует о.р. стратегия F_1, которая по любой функции $\psi\in U_1$ предельно синтезирует номер из $\mu(\psi)$.

<u>Шаг индукции</u>. Пусть $j\in\{1,2,3,\ldots\}$. Будем по индукции считать, что уже построены эффективно перечислимые классы $U_1,\ldots,U_j$ и они $\mu-\nu$ -синтезируемы о.р. стратегиями $F_1, F_2, \ldots, F_j$, притом, если $j>1$, то $F_1, F_2, \ldots, F_{j-1}$ -именно те стратегии, которые были использованы при определении классов $U_2, U_3, \ldots, U_j$. Будем по индукции считать также, что существует алгоритм $\mathfrak{A}_j$, который по произвольному φ -номеру произвольной стратегии F_j, предельно ν -синтезирующей класс U_j, и по канторовскому номеру p любого корте-

тежа $\{y_0, y_1, \ldots, y_m\}$ произвольной длины указывает φ-номер такой функции f что 1) f принимает значение $f(0)=y_0,\ f(1)=y_1, \ldots, f(m)=y_m$ 2) f принадлежит всем классам $U_1, U_2, \ldots, U_j$, и 3) стратегии $F_1, F_2, \ldots, F_j$ предельно синтезируют j различных номеров функции f (т.е. если $1 \leqslant u < v \leqslant j$, то F_u и F_v предельно синтезируют разные ν номера функции f). Разумеется, при $j=1$ существование такого алгоритма тривиально: в качестве f может быть взята функция $f(0)=y_0,\ f(1)=y_1, \ldots, f(m)=y_m,$ $f(m+1)=f(m+2)=\cdots=0.$

Класс U_{j+1} будет эффективно перечислимым классом о.р.функций $U_{j+1}=\{h_z(x)\}$. Начнем построение функций $h_z(x)$. Построение при каждом z будет проводиться по этапам. Во время каждого этапа будут определены значения функции $h_z(x)$ на некотором непустом отрезке натурального ряда, непосредственно примыкающем справа к тому отрезку, где функция была определена на предыдущем этапе. Кроме того, в результате каждого этапа будет определена некоторая функция f, называемая эталонной. Эта функция будет использована для определения значений функции $h_z(x)$ на следующем этапе конструкции.

Этап 0. Пусть $z=c(i,p)$ и $p=\langle y_0, y_1, \ldots, y_r\rangle$. Тогда определяем $h_z(0)=y_0,\ h_z(1)=y_1, \ldots, h_z(r)=y_r$. Если $p=0$, т.е. если p равен номеру пустого кортежа, то $h_z(0)=0$.

В качестве эталонной функции возьмем функцию f, номер которой выдает алгоритм $\mathfrak{A}_j$ по F_j и p.

Этап $S+1$. Пусть $z=c(i,p)$, $p=\langle y_0, y_1, \ldots, y_r\rangle$ и пусть g-функция из леммы 4.1. Предполагаем, что на предыдущих этапах определены значения $h_z(0), h_z(1), \ldots, h_z(k)$ так, что $k \geqslant r$ и $h_z(0)=y_0,\ h_z(1)=y_1, \ldots, h_z(r)=y_r$. Предположим также, что эталонная функция f выбрана таким образом, что 1) f принадлежит всем классам $U_1, U_2, \ldots, U_j$, 2) $h_z(0)=f(0),\ h_z(1)=f(1), \ldots, h_z(k)=f(k)$ и 3) никакие две из стратегий $F_1, F_2, \ldots, F_j$ не синтезируют в пределе один и тот же ν - номер функции f.

Для определения значения $h_z(k+1)$ мы будем параллельно вычислять: I) последовательности значений

$$F_1(\langle f(0),f(1),\dots,f(k)\rangle),\ F_1(\langle f(0),f(1),\dots,f(k+1)\rangle),\ F_1(\langle f(0),f(1),\dots,f(k+2)\rangle),\dots$$
$$F_2(\langle f(0),f(1),\dots,f(k)\rangle),\ F_2(\langle f(0),f(1),\dots,f(k+1)\rangle),\ F_2(\langle f(0),f(1),\dots,f(k+2)\rangle),\dots$$
- -
$$F_j(\langle f(0),f(1),\dots,f(k)\rangle),\ F_j(\langle f(0),f(1),\dots,f(k+1)\rangle),\ F_j(\langle f(0),f(1),\dots,f(k+2)\rangle),\dots$$
$$\varphi_{g(i)}(\langle f(0),f(1),\dots,f(k)\rangle),\ \varphi_{g(i)}(\langle f(0),f(1),\dots,f(k+1)\rangle),\ \varphi_{g(i)}(\langle f(0),f(1),\dots,f(k+2)\rangle),\dots$$

и 2) значение

$$\nu_{\varphi_{g(i)}(\langle f(0),f(1),\dots,f(k)\rangle)}^{(k+1)}.$$

Мы будем выполнять описываемую ниже цепь проверок, связанных с этими вычислениями. В результате каждой из таких проверок должен быть получен ответ "да" или "нет". В одном случае цепь проверок продолжается, в другом - обрывается. Опишем сначала эту цепь, а потом, как определить дальнейшие значения функции h_z и эталонную функцию, когда цепь обрывается.

Сначала проверяем, совпадают ли значения $\varphi_{g(i)}(\langle f(0),f(1),\dots,f(k)\rangle)$ и $\varphi_{g(i)}(\langle f(0),f(1),\dots,f(k+1)\rangle)$. Если совпадают, то выясняем, верно ли, что вычисление

$$\nu_{\varphi_{g(i)}(\langle f(0),f(1),\dots,f(k)\rangle)}^{(k+1)}$$

останавливается за I такт и дает результат $f(k+1)$. Если не останавливается или дает другой результат, то выясняем, существуют ли такие $r\in\{1,2,\dots,j\}$, что

$$F_r(\langle f(0),f(1),\dots,f(k)\rangle)=F_r(\langle f(0),f(1),\dots,f(k+1)\rangle).$$

Если существуют, то проверяем, отличается ли $\varphi_{g(i)}(\langle f(0),f(1),\dots,f(k+1)\rangle)$ одновременно от всех таких $F_r(\langle f(0),f(1),\dots,f(k+1)\rangle)$. Если отличается не от всех таких значений F_r, то проверяем, совпадают ли значения $\varphi_{g(i)}(\langle f(0),f(1),\dots,f(k+1)\rangle)$ и $\varphi_{g(i)}(\langle f(0),f(1),\dots,f(k+2)\rangle)$. Если совпадают, то выясняем, верно ли, что вычисление

$$\vartheta_{\varphi_{g(i)}}(\langle f(0), f(1), \dots, f(k)\rangle)^{(k+1)}$$

останавливается за 2 такта и дает результат $f(k+1)$. Если не останавливается или дает другой результат, то выясняем, существуют ли такие $r \in \{1, 2, \dots, j\}$, что
$F_r(\langle f(0), f(1), \dots, f(k)\rangle) = F_r(\langle f(0), f(1), \dots, f(k+1)\rangle) = F_r(\langle f(0), f(1), \dots, f(k+2)\rangle)$.
Если существуют, то проверяем, отличается ли $\varphi_{g(i)}(\langle f(0), f(1), \dots, f(k+2)\rangle)$ одновременно от всех таких $F_r(\langle f(0), f(1), \dots, f(k+2)\rangle)$. Если отличается не от всех таких значений F_r , то проверяем, совпадают ли значения $\varphi_{g(i)}(\langle f(0), f(1), \dots, f(k+2)\rangle)$ и $\varphi_{g(i)}(\langle f(0), f(1), \dots, f(k+3)\rangle)$, и т.д.

Эта цепь проверок может оборваться по четырем причинам, и мы эти причины будем различать:

а) может оказаться, что закончилось вычисление

$$\vartheta_{\varphi_{g(i)}}(\langle f(0), f(1), \dots, f(k)\rangle)^{(k+1)} = f(k+1),$$

б)может оказаться, что существует такое m , что

$$\varphi_{g(i)}(\langle f(0), f(1), \dots, f(m-1)\rangle) \neq \varphi_{g(i)}(\langle f(0), f(1), \dots, f(m)\rangle),$$

в) может оказаться, что существует такое $m > k$, что не существует таких $r \in \{1, 2, \dots, j\}$, при которых

$$F_r(\langle f(0), f(1), \dots, f(k)\rangle) = F_r(\langle f(0), f(1), \dots, f(k+1)\rangle) = \dots = F_r(\langle f(0), f(1), \dots f(m)\rangle),$$

г) может оказаться, что существует такое $m > k$, что $\varphi_{g(i)}(\langle f(0), f(1), \dots, f(m)\rangle)$ отличается от всех тех $F_r(\langle f(0), f(1), \dots, f(m)\rangle)$ $(r \in \{1, 2, \dots, j\})$, что
$F_r(\langle f(0), f(1), \dots, f(k)\rangle) = F_r(\langle f(0), f(1), \dots, f(k+1)\rangle) = \dots = F_r(\langle f(0), f(1), \dots, f(m)\rangle)$

В ситуации а) мы определяем $h_z(k+1) = f(k+1) + 1$ и находим новую эталонную функцию, пользуясь алгоритмом $\mathfrak{A}_j$, работающим на F_j и канторовском номере кортежа

$$\{h_z(0), h_z(1), \dots, h_z(k+1)\}.$$

В ситуациях б), в), г) определяем $h_2(k+1)=f(k+1)$, $h_2(k+2)=f(k+2), \ldots, h_2(m)=f(m)$ и в качестве эталонной функции оставляем ту же самую f.

Этим описание этапа $s+1$ завершено. Далее выполняется этап $s+2$.

Докажем теперь, что каждый этап должен когда-нибудь завершиться. Для этого достаточно показать, что при любых j и s упомянутая выше цепь проверок должна оборваться. Действительно, эталонная функция f принадлежит всем классам $U_1, U_2, \ldots, U_j$. Стратегии $F_1, F_2, \ldots, F_j$ предельно ν-синтезируют эти классы. Значит, все эти стратегии предельно синтезируют функцию f правильно. Если бы цепь проверок никогда не кончилась, то это означало бы, что $\varphi_{g(i)}(\langle f(0), f(1), \ldots, f(k)\rangle) = \varphi_{g(i)}(\langle f(0), f(1), \ldots, f(k+1)\rangle) =$

$= \ldots = \lim\limits_{n\to\infty} \varphi_{g(i)}(\langle f(0), f(1), \ldots, f(n)\rangle)$. Это означало бы также, что существует хотя бы одно такое $r \in \{1, 2, \ldots, j\}$, что $F_r(\langle f(0), f(1), \ldots, f(k)\rangle) = F_r(\langle f(0), f(1), \ldots, f(k+1)\rangle) =$

$= \ldots = \lim\limits_{n\to\infty} F_r(\langle f(0), f(1), \ldots, f(n)\rangle) = \lim\limits_{n\to\infty} \varphi_{g(i)}(\langle f(0), f(1), \ldots, f(n)\rangle)$.

Но тогда $\varphi_{g(i)}(\langle f(0), f(1), \ldots, f(k)\rangle)$ было бы ν-номером функции f, и, следовательно,

$$\nu_{\varphi_{g(i)}(\langle f(0), f(1), \ldots, f(k)\rangle)}(k+1) = f(k+1).$$

Докажем теперь, что при любых i и p функция $h_{c(i,p)}$ обладает следующими свойствами:

А) Пусть $p = \langle y_0, y_1, \ldots, y_r \rangle$. Тогда $h_{c(i,p)}(0) = y_0,\ h_{c(i,p)}(1) = y_1, \ldots, h_{c(i,p)}(r) = y_r$.

Б) Если стратегия φ_i предельно ν-синтезирует функцию $h_{c(i,p)}$, то $h_{c(i,p)}$ принадлежит всем классам $U_1, U_2, \ldots, U_j, U_{j+1}$.

В) Если стратегия φ_i предельно ν-синтезирует функцию $h_{c(i,p)}$, то все стратегии $F_1, F_2, \ldots, F_j, \varphi_i$ предельно синтезируют различные ν-номера этой функции.

Свойство А) вытекает из конструкции очевидным образом. Докажем остальные свойства.

Конструкция $h_{c(i,p)}$ состоит из отдельных этапов. Каждый из них когда-нибудь завершается одной из четырех ситуаций а), б), в), г). Хотя бы один из этих типов ситуаций должен повторяться бесконечно много раз. Возможны такие случаи:

I) ситуация а) повторяется бесконечно много раз.

Тогда φ_i не может предельно ν -синтезировать функцию $h_{c(i,p)}$, ибо делает на ней бесконечно много ошибок.

2) ситуация б) повторяется бесконечно много раз.

Тогда φ_i не может предельно ν -синтезировать функцию $h_{c(i,p)}$, ибо бесконечно много раз меняет свое значение.

3) ситуация а) и б) повторяются только конечное число раз.

Тогда, начиная с некоторого этапа, эталонная функция не меняется, и $h_{c(i,p)}$ совпадает с этой эталонной функцией, и, следовательно, принадлежит $U_1, U_2, \dots, U_j$. Свойство Б) доказано.

Каждая из стратегий $F_1, F_2, \dots, F_j$ на эталонной функции меняет значение только конечное число раз, притом пределы значений этих стратегий различны. Если φ_i тоже меняет значение на $h_{c(i,p)}$ только конечное число раз, то все этапы с достаточно большими номерами могут окончиться толко ситуацией г). Отсюда вытекает свойство В).

Для завершения шага индукции остается заметить, что алгоритм $\mathfrak{A}_{j+1}$ по номеру i стратегии φ_i и номеру p кортежа $\{y_0, y_1, \dots, y_n\}$ может выдать φ-номер функции $h_{c(i,p)}$.

Завершим теперь доказательство теоремы.

Пусть c - произвольное натуральное число и пусть φ_i -стратегия, предельно μ-ν -синтезирующая класс U_{c+1}. Рассмотрим функцию $h_{c(i,0)}$ из класса U_{c+1}. Так как эта функция принадлежит также классам $U_1, U_2, \dots, U_c$, то стратегии $F_1, F_2, \dots, F_c$ правильно предельно μ-ν -синтезируют функцию $h_{c(i,0)}$. Но по определению этой функции стратегии $F_1, F_2, \dots, F_c, \varphi_i$ предельно μ-ν -синтезируют попарно различные номера функции $h_{c(i,0)}$. Следовательно, фиксация μ не может быть c -ограниченной.

СЛЕДСТВИЕ. Пусть c - произвольное натуральное число и пусть ν - такая вычислимая нумерация всех ч.р. функций, в которой каждая о.р. функция имеет не более чем c различных номеров. Тогда существует эффективно перечислимый класс U о.р. функций, который не является предельно ν -синтезируемым.

С теоремой 4 контрастирует следующая теорема.

ТЕОРЕМА 5. Для любой вычислимой нумерации ν всех ч.р. функций существует такая фиксация ν -номеров μ, что I) для любой о.р. функции f множество $\mu(f)$ является конечным, и 2) для любого класса о.р. функций из предельной ν -синтезируемости вытекает предельная μ-ν -синтезируемость.

ЛЕММА 5.I. Пусть ν - произвольная нумерация всех ч.р. функций, U - предельно ν -синтезируемый класс о.р. функций, U' - класс, состоящий из конечного числа о.р. функций, и μ -произвольная фиксация ν -номеров всех функций класса U'. Тогда существует ч.р. стратегия σ, которая одновременно: I) предельно ν - синтезирует класс U, 2) предельно μ-ν - синтезирует класс U'.

ДОКАЗАТЕЛЬСТВО. Пусть σ' - ч.р. стратегия, предельно ν-синтезирующая класс U. Если U' - пустой класс, то в качестве σ может быть взята сама стратегия σ'. Пусть $U' = \{f_0, f_1, \ldots, f_n\}$. Тогда стратегия σ работает следующим образом. Для нее не представляет труда "запомнить" по одному номеру из $\mu(f_i)$ для каждой функции f_i $(i = 0, 1, \ldots, n)$ класса U'. Обозначим эти выделенные номера через $j_0, j_1, \ldots, j_n$. Работая на произвольной о.р. функции f, стратегия σ выдает значение j_0 до тех пор, пока не выяснилось, что $f \neq f_0$, потом выдает j_1 до тех пор, пока не выявилось, что $f \neq f_1$, ..., потом выдает j_n до тех пор, пока не выяснилось, что $f \neq f_n$. Когда уже таким образом выявилось, что $f \notin U'$, стратегия σ начинает выдавать то же самое значение, что и стратегия σ'.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 5. Пусть $\{f_0, f_1, f_2, \ldots\}$ произвольная однозначная нумерация всех о.р. функций. (Эта нумерация, конечно, не может быть вычислимой.)

Каждая ч.р. функция φ_i, используемая как стратегия, предельно ν-синтезирует некоторый (быть может пустой) класс о.р. функций. Будем индукцией по i (неэффективно) перестраивать каждую стратегию φ_i в ч.р. стратегию $\varphi_{h(i)}$, предельно ν- синтезирующую не меньше о.р. функций, чем стратегия φ_i, и одновременно будем строить требуемую фиксацию μ.

Для базиса индукции определим $\varphi_{h(0)}$ равной φ_0. Если стратегия φ_0 предельно синтезирует ν-номер функции f_0 правильно, то $\mu(f_0)$ определим как множество, состоящее из того номера функции f_0, который предельно синтезирует φ_0. В противном случае $\mu(f_0)$ определяется как множество, состоящее из какого-то одного ν-номера функции f_0, например, минимального.

Пусть уже определены $\varphi_{h(0)}, \varphi_{h(1)}, \ldots, \varphi_{h(j)}$ и $\mu(f_0), \mu(f_1), \ldots, \mu(f_j)$. Функцию $\varphi_{h(j+1)}$ определим как стратегию σ из леммы 5.I, если в ней в качестве U взят класс, предельно ν-синтезируемый стратегией φ_{j+1}, а в качестве U' - класс $\{f_0, f_1, \dots, f_j\}$. Потом $\mu(f_{j+1})$ определяется как множество, состоящее из всех тех ν-номеров функции f_{j+1}, которые предельно синтезируются хотя бы одной из стратегий $\varphi_{h(0)}, \varphi_{h(1)}, \dots, \varphi_{h(j)}$ (точнее, одной из тех указанных стратегий, которые предельно синтезируют правильный ν-номер функции f_{j+1}). Если в результате такого определения $\mu(f_{j+1})$ оказывается пустым, то переопределяем $\mu(f_{j+1})$ как множество, состоящее из минимального ν-номера функции f_{j+1}.

Легко видеть, что определенная таким образом фиксация ν-номеров всех о.р. функций μ сопоставляет каждой о.р. функции только конечное множество номеров. Если некоторый класс о.р.функций предельно ν-синтезируем стратегией φ_i, то он предельно μ-ν-синтезируем стратегией $\varphi_{h(i)}$.

СЛЕДСТВИЕ. Пусть φ - главная вычислимая нумерация всех ч.р. функций. Тогда существует такая фиксация φ-номеров μ, что I) для любой о.р. функции f множество $\mu(f)$ является конечным, и 2) любой эффективно перечислимый класс предельно μ-φ-синтезируем.

При сопоставлении следствий теорем 4 и 5 возникает следующий вопрос: существует ли такая вычислимая нумерация ν всех одноместных ч.р. функций, что I) каждая о.р. одноместная функция в ней имеет только конечное число номеров, и 2) любой эффективно перечислимый класс о.р. функций является предельно ν-синтезируемым. Этот вопрос остается открытым.

В заключение рассмотрим одно утверждение, имеющее определенное отношение к поставленному вопросу.

ТЕОРЕМА 6. Пусть φ - главная вычислимая нумерация всех одноместных ч.р. функций. Существует такая вычислимая нумерация ν всех одноместных ч.р. функций, что I) бесконечно много различных о.р. функций имеют в нумерации ν только по одному номеру, и 2) любой предельно φ -синтезируемый класс о.р. функций является предельно ν - синтезируемым.

ДОКАЗАТЕЛЬСТВО. Нумерация ν определяется следующим образом. Если $n=2m+1$, то функция ν_n - это константа m. Если $n=2m$ и $m=c(i,j)$, то

$$\nu_n(x)=\begin{cases}\varphi_i(x), & \text{если } x\neq j\\ \varphi_i(j), & \text{если } x=j \text{ и } \varphi_i \text{ в своей области определения принимает хотя бы два различных значения.}\end{cases}$$

Очевидно, любая константная функция имеет в нумерации ν только один номер. Если φ_i принимает хотя бы два различных значения, то $\nu_{2\cdot c(i,0)}=\varphi_i$. Если φ_i доопределима до некоторой константы, но не определена в какой-то точке j, то $\varphi_i=\nu_{2\cdot c(i,j)}$. Следовательно, ν - нумерация всех одноместных ч.р. функций.

Если стратегия φ_k предельно φ -синтезирует некоторый класс U о.р. функций, то класс U предельно ν - синтезируем следующей стратегией $\varphi_{h(k)}$:

$$\varphi_{h(k)}(x)=\begin{cases}2m+1, & \text{если } x=\langle m,m,\dots,m\rangle\\ 2\cdot c(\varphi_k(x),0), & \text{если } x \text{ - номер неконстантного кортежа.}\end{cases}$$

Основные результаты статьи опубликованы без доказательства в [I2].

Автор выражает благодарность Я.М.Барздиню за постоянное внимание к работе.

ЛИТЕРАТУРА

1. Barzdin J.M. Prognostication of automata and functions. - Information Processing 71, North-Holland, 1972.
2. Барздинь Я.М., Фрейвалд Р.В. Прогнозирование общерекурсивных функций. - ДАН СССР, 1972, т.206, №3.
3. Барздинь Я.М., Подниекс К.М. К теории индуктивного вывода.-Труды симпозиума "Mathematical foundations of computer science", High Tatras. Czechoslovakia, 1973.
4. "Учен. зап. Латв. ун-та. Теория алгоритмов и программ. I", 1974, т. 210.
5. Ершов Ю.Л. Теория нумераций. I. Новосибирск, НГУ, 1969.
6. Friedberg R.M. Three theorems on recursive functions: I Decomposition. II Maximal sets. III Enumeration without duplication.- J.Symbolic Logic, 23, 1958, 309-318.
7. Gold E.M. Limiting recursion.-"Journal of Symbolic Logic", 1965, No 1.
8. Gold E.M. Language identification in the limit. - "Information and Control", 1967, v.10, No5.
9. Трахтенброт Б.А. Оптимальные вычисления и частотное явление Яблонского.- "Алгебра и Логика. Семинар" 1965, т.4, №5.
10. Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. М., 1972.
11. Кинбер Е.Б. О предельном синтезе почти минимальных геделевских номеров. -"Учен. зап. Латв. ун-та", 1974. т. 210.
12. Фрейвалд Р.В. О предельном синтезе номеров общерекурсивных функций в различных вычислимых нумерациях.- ДАН СССР, 1974, т. 219, № 4.

СООТНОШЕНИЯ МЕЖДУ ПРОГНОЗИРУЕМОСТЬЮ И ПРЕДЕЛЬНОЙ СИНТЕЗИРУЕМОСТЬЮ

Р.В.Фрейвалд, Я.М.Барздинь

Пусть зафиксированы произвольная геделевская (т.е. главная вычислимая) нумерация φ всех одноместных частично рекурсивных (ч.р.) функций и канторовская нумерация $\langle x_1, x_2, \ldots, x_n \rangle$ всех конечных кортежей натуральных чисел. Общерекурсивные (о.р.) функции, осуществляющие взаимно однозначное соответствие между парами натуральных чисел и натуральными числами, будем обозначать через $c(x,y)$, $l(u)$, $r(u)$. Стратегией будем называть произвольную двуместную ч.р. функцию.

ОПРЕДЕЛЕНИЕ 1. Говорят, что стратегия F прогнозирует функцию f на последовательности натуральных чисел $\Omega = \{x_0, x_1, x_2, \ldots\}$, если: 1) для любого натурального n значение $F(\langle x_0, x_1, \ldots, x_n, x_{n+1} \rangle, \langle f(x_0), f(x_1), \ldots, f(x_n) \rangle)$ определено, и 2) для всех n (кроме конечного числа)

$$F(\langle x_0, x_1, \ldots, x_n, x_{n+1} \rangle, \langle f(x_0), f(x_1), \ldots, f(x_n) \rangle) = f(x_{n+1}).$$

ОПРЕДЕЛЕНИЕ 2. Говорят, что стратегия F предельно φ-синтезирует функцию f на последовательности натуральных чисел $\Omega = \{x_0, x_1, x_2, \ldots\}$, если: 1) для любого натурального n значение $F(\langle x_0, x_1, \ldots, x_n \rangle, \langle f(x_0), f(x_1), \ldots, f(x_n) \rangle)$ определено, и 2) предел

$$\lim_{n \to \infty} F(\langle x_0, x_1, \ldots, x_n \rangle, \langle f(x_0), f(x_1), \ldots, f(x_n) \rangle)$$

существует и равен некоторому φ-номеру функции f или другой функции, которая на элементах последовательности Ω не отличима от f.

ОПРЕДЕЛЕНИЕ 3. Говорят, что класс U о.р.функций прогнозируем (соответственно: предельно φ -синтезируем) на последовательности натуральных чисел $\Omega=\{x_0,x_1,x_2,\dots\}$ если существует стратегия F , которая прогнозирует (предельно φ - синтезирует) на Ω все функции класса U .

ОПРЕДЕЛЕНИЕ 4. Говорят, что класс U о.р. функций прогнозируем (предельно φ -синтезируем) равномерно на всех последовательностях натуральных чисел, если существует стратегия F , которая прогнозирует (предельно φ - синтезирует) все функции класса U на всевозможных последовательностях натуральных чисел Ω .

Очевидно, что если φ' и φ'' - две геделевские нумерации, то предельная φ'-синтезируемость эквивалентна предельной c''-синтезируемости. Поэтому обозначение конкретной геделевской нумерации мы будем опускать и будем говорить просто о предельной синтезируемости.

Эти понятия были впервые исследованы нами в [I] . Однако там было сформулировано неверное утверждение, будто равномерные на всех последовательностях натуральных чисел прогнозируемость и предельная синтезируемость совпадают. (М.Блюм также обратил внимание авторов на неверность этого утверждения.) Следующие теоремы исправляют эту ошибку и дают довольно полную характеристику соотношений между прогнозируемостью и синтезируемостью

ТЕОРЕМА I. Существует класс о.р. функций, который предельно синтезируем равномерно на всех последовательностях натуральных чисел,но не прогнозируем на $\Omega_0=\{0,1,2,3,\dots\}$

В доказательстве теоремы нам понадобится следующая лемма, впервые сформулированная в явном виде в учебнике Б.А.Трахтенброта [3] при изложении теоремы М.Блюма об ускорении [4] .

ЛЕММА. Пусть $g(i)$ - о.р. функция. Если для любого i всегда одновременно выполняются оба следующих свойства:

I) $\varphi_{g(i)}(0)$ определено,

2) если при некотором x оказывается, что $\varphi_i(0)$, $\varphi_i(1), \ldots$ $\ldots, \varphi_i(x)$ определены, то определены также $\varphi_{g(i)}(0), \varphi_{g(i)}(1), \ldots$ $\ldots, \varphi_{g(i)}(x)$, $\varphi_{g(i)}(x+1)$,

то каждая неподвижная точка i_0 функции $g(i)$ $(\varphi_{i_0} = \varphi_{g(i_0)})$ является номером о.р.функции.

ДОКАЗАТЕЛЬСТВО очевидно.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ I. Рассмотрим класс U, который состоит из всевозможных таких о.р.функций $f(x)$, что: I) для каждого x значение $\ell(f(x))$ является номером в геделевской нумерации φ такой ч.р.функции $\psi(t)$, что значение $\psi(0), \psi(1), \psi(2), \ldots, \psi(x)$ определены и равны соответствующим значениям функции f, и 2) существует предел $\lim\limits_{x\to\infty} \ell(f(x))$.[ж)]

I. Класс U предельно синтезируем равномерно на всех последовательностях натуральных чисел следующей стратегией

$$F(\langle x_0, x_1, \ldots, x_n\rangle, \langle f(x_0), f(x_1), \ldots, f(x_n)\rangle) = \ell(f(\max\{x_0, x_1, \ldots, x_n\})).$$

2. Докажем, что класс U не прогнозируем на Ω_0. Допустим от противного, что стратегия F прогнозирует класс U на Ω_0. Возможны два случая: существуют или не существуют такие числа $n, y_0, y_1, \ldots, y_n$, что а) для любого $k \in \{0, 1, 2, \ldots, n\}$ значение $\ell(y_k)$ является номером в геделевской нумерации φ такой ч.р.функции $\psi(t)$, что $\psi(0) = y_0$, $\psi(1) = y_1, \ldots, \psi(k) = y_k$ и б) значение $F(\langle 0, 1, \ldots, k, k+1\rangle, \langle y_0, y_1, \ldots, y_k\rangle)$ не определено.

Пусть такие числа существуют. Убедимся, что класс U содержит функцию f, принимающую значения

ж) Наш класс U построен, развивая одну идею Р.Р. Витковского.

$f(0)=y_0,\ f(1)=y_1, \ldots, f(n)=y_n$ – этим будет доказано, что стратегия F не прогнозирует некоторую функцию из класса U. Действительно, сопоставим каждому натуральному числу i функцию

$$\varphi_{h(i)}(x)=\begin{cases} y_x & , \text{если } x \leq n \\ c(i,0) & , \text{если } x > n \end{cases}$$

По теореме о неподвижной точке [5] существует такое j, что

$$\varphi_j(x)=\begin{cases} y_x & , \text{если } x \leq n \\ c(j,0) & , \text{если } x > n \end{cases}$$

Это противоречит допущению, что стратегия F прогнозирует класс U.

Рассмотрим теперь другой случай: когда для стратегии F чисел $n, y_0, y_1, \ldots, y_n$ со свойствами а) и б) не существует.

Для каждого натурального i эффективно определим функцию $\varphi_{g(i)}(x)$. Сначала полагаем $\varphi_{g(i)}(0)=c(i,0)$. Далее начинаем вычислять $\varphi_i(0)$. Если на самом деле $\varphi_i(0)$ не определено, то $\varphi_{g(i)}(1), \varphi_{g(i)}(2), \varphi_{g(i)}(3), \ldots$ окажутся не определенными. Пусть вычисление $\varphi_i(0)$ закончилось. Если оказывается, что $\varphi_i(0)\neq c(i,0)$ (т.е. если $\varphi_i(0)\neq\varphi_{g(i)}(0)$), то полагаем $\varphi_{g(i)}(1)=\varphi_{g(i)}(2)=\cdots=c(i,0)$. Если оказывается, что $\varphi_i(0)=c(i,0)=\varphi_{g(i)}(0)$, то определяем $\varphi_{g(i)}(1)=c(i,\overline{sg}\ r(F(\langle 0,1\rangle,\langle\varphi_{g(i)}(0)\rangle)))$.

Заметим, что $\varphi_{g(i)}(1)$ определено, так как по предположению для стратегии F чисел $n, y_0, y_1, \ldots, y_n$ с упомянутыми выше свойствами а) и б) не существует. Для чисел $n=1,\ y_0=c(i,0)$ свойство а) выполнено, следовательно, свойство б) нарушается и $F(\langle 0,1\rangle,\langle\varphi_{g(i)}(0)\rangle)$ должно быть определено.

Итак, пусть $\varphi_{g(i)}(1)$ вычислено. Далее начинаем вычислять $\varphi_i(1)$. Если на самом деле $\varphi_i(1)$ не определено, то $\varphi_{g(i)}(2), \varphi_{g(i)}(3), \varphi_{g(i)}(4), \dots$ окажутся не определенными. Пусть вычисление $\varphi_i(1)$ закончилось. Если оказывается, что $\varphi_i(1) \neq \varphi_{g(i)}(1)$, то полагаем $\varphi_{g(i)}(2) = \varphi_{g(i)}(3) = \varphi_{g(i)}(4) = \dots = c(i,0)$. Если оказывается, что $\varphi_i(1) = \varphi_{g(i)}(1)$, то определяем $\varphi_{g(i)}(2) = c(i, \overline{sg}\, r(F(\langle 0,1,2\rangle, \langle \varphi_{g(i)}(0), \varphi_{g(i)}(1)\rangle)))$. (Из предположения о стратегии F вытекает, что и это значение должно быть определено).

После этого начинаем вычислять $\varphi_i(2)$. Если $\varphi_i(2) \neq \varphi_{g(i)}(2)$, то $\varphi_{g(i)}(3) = \varphi_{g(i)}(4) = \dots = c(i,0)$. Если $\varphi_i(2) = \varphi_{g(i)}(2)$, то

$$\varphi_{g(i)}(3) = c(i, \overline{sg}\, r(F(\langle 0,1,2,3\rangle, \langle \varphi_{g(i)}(0), \varphi_{g(i)}(1), \varphi_{g(i)}(2)\rangle))) \quad \text{и т.д.}$$

По теореме о неподвижной точке существует такое j, что $\varphi_j = \varphi_{g(j)}$. Условия леммы выполнены, следовательно, $\varphi_j = \varphi_{g(j)}$ –о.р. функция. Так как для всех натуральных n имеет место $\varphi_j(n) = \varphi_{g(j)}(n)$, то по конструкции функции $\varphi_{g(j)}$ для всех натуральных n

$$\varphi_{g(j)}(n+1) \neq F(\langle 0,1,2,\dots,n,n+1\rangle, \langle \varphi_{g(j)}(0), \varphi_{g(j)}(1), \dots, \varphi_{g(j)}(n)\rangle).$$

Таким образом, стратегия F не прогнозирует функцию $\varphi_{g(j)}$. Но функция $\varphi_{g(j)}$ принадлежит классу U, так как для всех x $\ell(\varphi_{g(j)}(x)) = j$ и $\varphi_j = \varphi_{g(j)}$. Противоречие. Теорема доказана.

Теорема I показывает, что понятия прогнозируемости и предельной синтезируемости отличаются весьма значительно. Тем не менее прогнозируемость равномерно на всех последовательностях натуральных чисел можно адекватно описать только в терминах предельной синтезируемости (см.теорему 2 ниже).

ОПРЕДЕЛЕНИЕ 5. Будем говорить, что стратегия F предельно φ-тотально-синтезирует функцию f на последовательности натуральных чисел $\Omega = \{x_0, x_1, x_2, \dots\}$, если:
I) для любого натурального n значение

$$F(\langle x_0, x_1, \dots, x_n\rangle, \langle f(x_0), f(x_1), \dots, f(x_n)\rangle)$$

определено и равно φ-номеру некоторой общерекурсивной функции, и 2) предел

$\lim\limits_{n\to\infty} F(\langle x_0, x_1, \dots, x_n\rangle, \langle f(x_0), f(x_1), \dots, f(x_n)\rangle)$ существует и равен некоторому φ-номеру функции f или другой функции, которая на элементах последовательности Ω не отличима от f.

Для введения понятий "класс функций предельно φ-тотально-синтезируем на последовательности Ω" и "класс функций предельно φ-тотально-синтезируем равномерно на всех последовательностях натуральных чисел" используются определения, аналогичные приведенным выше определениям 3 и 4. Введенные таким образом понятия снова оказываются инвариантными относительно выбора конкретной геделевской нумерации. Поэтому везде ниже мы будем опускать обозначение нумерации и будем говорить просто о предельной тотально-синтезируемости в том или ином смысле.

ТЕОРЕМА 2. Любой класс о.р. функций прогнозируем равномерно на всех последовательностях натуральных чисел тогда и только тогда, когда он предельно тотально-синтезируем равномерно на всех последовательностях натуральных чисел.

ДОКАЗАТЕЛЬСТВО. $\Longleftarrow$ Не представляет труда.

$\Longrightarrow$ Пусть стратегия F прогнозирует данный класс U равномерно на всех последовательностях натуральных чисел. Пусть φ, как и раньше, геделевская нумерация всех одноместных ч.р. функций. Рассмотрим следующую стратегию G и покажем, что она предельно φ-тотально-синтезирует класс U.

Значение стратегии G на паре номеров пустого кортежа $G(\langle\varnothing\rangle, \langle\varnothing\rangle)$ равно φ-номеру следующей функции

$$h(x)=F(\langle x\rangle,\langle \varnothing\rangle).$$

Значение стратегии G на других парах номеров кортежей определяется следующим образом.
Если

$$\varphi_{G(\langle x_0,x_1,\dots,x_{n-1}\rangle,\langle y_0,y_1,\dots,y_{n-1}\rangle)}(x_n)=y_n,$$

то $G(\langle x_0,x_1,\dots,x_n\rangle,\langle y_0,y_1,\dots,y_n\rangle)=G(\langle x_0,x_1,\dots,x_{n-1}\rangle,\langle y_0,y_1,\dots,y_{n-1}\rangle)$.

В противном случае выделяем все те $n_1,n_2,\dots,n_t$, для которых

$$\varphi_{G(\langle x_0,x_1,\dots,x_{n_i-1}\rangle,\langle y_0,y_1,\dots,y_{n_i-1}\rangle)}(x_n)=y_n,$$

и определяем $G(\langle x_0,x_1,\dots,x_n\rangle,\langle y_0,y_1,\dots,y_n\rangle)$ равным φ - номеру следующей функции

$$h(x)=\begin{cases} y_{n_i}, & \text{если } x=x_{n_i}\ (i\in\{1,2,\dots,t\}) \\ F(\langle x_0,x_{n_1},x_{n_2},\dots,x_{n_t},x\rangle,\langle y_0,y_{n_1},y_{n_2},\dots,y_{n_t}\rangle), & \text{для остальных } x. \end{cases}$$

Если класс U содержит функцию f, принимающую значения $f(x_0)=y_0,\ f(x_1)=y_1,\dots,f(x_n)=y_n$, то значение $G(\langle x_0,x_1,\dots,x_n\rangle,\langle y_0,y_1,\dots,y_n\rangle)$ является номером о.р. функции, так как стратегия F прогнозирует класс U равномерно на всех последовательностях натуральных чисел.

Для завершения доказательства теоремы допустим от противного, что существуют последовательность $\Omega=\{x_0,x_1,x_2,\dots\}$ и функция $f\in U$, такие что стратегия G не синтезирует предельно f на Ω, т.е. меняет на ней значение бесконечно много раз.

Пусть $\Omega' = \{\zeta_0, \zeta_1, \zeta_2, \dots\}$ -подпоследовательность последовательности Ω, содержащая все те элементы x_n, при которых

$$G(\langle x_0,x_1,\dots,x_n\rangle,\langle f(x_0),f(x_1),\dots,f(x_n)\rangle) \neq G(\langle x_0,x_1,\dots,x_{n-1}\rangle,\langle f(x_0),f(x_1),\dots,f(x_{n-1})\rangle)$$

Следовательно, Ω' -бесконечная последовательность.

Заметим, что, во-первых, последовательность Ω' обязательно бесповторная. Во-вторых, для всех t

$$f(\zeta_{t+1}) \neq F(\langle \zeta_0,\zeta_1,\zeta_2,\dots,\zeta_t,\zeta_{t+1}\rangle,\langle f(\zeta_0),f(\zeta_1),f(\zeta_2),\dots,f(\zeta_t)\rangle).$$

Но это означает, что стратегия F не прогнозирует функцию f на последовательности Ω'. Противоречие. Теорема доказана.

Итак, мы доказали, что в равномерном случае прогнозируемость эквивалентна предельной тотально-синтезируемости. Достаточно любопытно, что на Ω_0' (и на многих других последовательностях тоже) эти понятия все же отличаются. Из предельной тотально-синтезируемости некоторого класса U на Ω_0, конечно, вытекает прогнозируемость этого класса на Ω_0. Однако справедлива следующая теорема.

ТЕОРЕМА 3. Существует класс о.р. функций, который прогнозируем на $\Omega_0 = \{0,1,2,3,\dots\}$, но не предельно тотально - синтезируем на Ω_0.

ДОКАЗАТЕЛЬСТВО. Рассмотрим класс U, который состоит из всевозможных таких о.р. функций $f(x)$, что: I) для каждого x значение $\ell(f(x))$ является номером в геделевской нумерации φ такой ч.р. функции $\psi(t)$, что $\psi(0) = f(0)$, $\psi(1) = f(1), \dots, \psi(x) = f(x)$ и $\psi(x+1)$ определено, но не обязательно равно $f(x+1)$ и 2) существует предел $\lim\limits_{x\to\infty} \ell(f(x))$

I. Класс U прогнозируем на Ω_0 следующей стратегией

$$F(\langle 0,1,\ldots,x,x+1\rangle, \langle f(0), f(1),\ldots,f(x)\rangle) = \varphi_{\ell(f(x))}$$

2. Докажем, что класс U не является предельно тотально-синтезируемым на Ω_0. Для этого нам потребуется следующее вспомогательное понятие.

Будем говорить, что стратегия G прогнозирует-с-пропуском функцию f на последовательности Ω_0, если: I) для любого натурального n значение $G(\langle f(0), f(1),\ldots,f(n)\rangle)$ определено, и 2) для всех n (кроме конечного числа) $G(\langle f(0), f(1),\ldots,f(n)\rangle) = f(n+2)$.

Легко видеть, что если некоторый класс о.р.функций предельно тотально-синтезируем на Ω_0, то существует стратегия G, прогнозирующая-с-пропуском все функции этого класса на Ω_0. Почти дословно повторяя второй пункт доказательства теоремы I, можно доказать, что для нашего класса U такой стратегии G не может быть.

Теорема 2 принадлежит Я.М.Барздиню и Р.В.Фрейвалду, остальные теоремы - Р.В.Фрейвалду.

Авторы выражают благодарность М.Блюму, который любезно указал на ошибку в [I].

ЛИТЕРАТУРА

I. Барздинь Я.М., Фрейвалд Р.В. Прогнозирование общерекурсивных функций.- ДАН СССР, 1972, т.206, № 3.
2. Подниекс К.М. Сравнение различных типов предельного синтеза и прогнозирования функций.- "Учен. зап. Латв. ун-та",1974. т.210.
3. Трахтенброт Б.А. Сложность алгоритмов и вычислений. Новосибирск, НГУ, 1967.
4. Блюм М. Машинно-независимая теория сложности рекурсивных функций.-В кн.: Проблемы математической логики М., 1970.
5. Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. М., 1972.

СРАВНЕНИЕ РАЗЛИЧНЫХ ТИПОВ ПРЕДЕЛЬНОГО СИНТЕЗА И ПРОГНОЗИРОВАНИЯ (СТАТЬЯ ВТОРАЯ)

К.М.Подниекс

Эта статья завершает [I] . Напомним определения. $\{\varphi_i\}$ - фиксированная геделевская нумерация всех 1-местных частично рекурсивных (ч.р.) функций. Всюду определенную функцию φ можно представить как последовательность её значений:

$$\varphi(0),\ \varphi(1),\ \ldots,\ \varphi(n),\ \ldots \qquad (*)$$

Поэтому понятны следующие обозначения функций и операций над функциями:

$$0^\infty,\quad ij\varphi,\quad 0^k 1^\infty,$$
$$0\,\varphi(0)\,0\,\varphi(1)\,0\,\varphi(2)\,0\ldots$$

К л а с с а м и называются только классы 1-местных общерекурсивных (о.р.) функций, R -класс всех таких функций. Символ $\subset$ означает строгое включение, $\subseteq$ - нестрогое. Через $\langle x_1 \ldots x_n \rangle$ обозначена фиксированная эффективная нумерация всех конечных кортежей натуральных чисел (в качестве номеров использованы в с е натуральные числа).

С т р а т е г и е й называется любая ч.р.функция. Особо выделяются о.р. стратегии.

I. П р е д е л ь н ы й с и н т е з. По данной последовательности (*) требуется выявить (в каком-то смысле) закон ее становления. Если F - стратегия, φ -функция, то значения $F(\langle \varphi(0) \ldots \varphi(n) \rangle)$ при $n = 0, 1, 2, \ldots$ называются г и п о т е з а м и. Гипотеза верна, если она - геделев номер функции φ.

Говорят, что F синтезирует класс U в смысле GN, если F - о.р. стратегия, и для любой $\varphi \in U$ последовательность гипотез $F(\langle \varphi(0) \dots \varphi(n) \rangle)$ стабилизируется на верной гипотезе. Через GN обозначим семейство классов:

$$\{ U | \exists F \, (F \text{ синтезирует } U \text{ в смысле } GN) \}.$$

Говорят, что F синтезирует класс U в смысле GN^{∞}, если F - о.р.стратегия, и для любой $\varphi \in U$ последовательность гипотез $F(\langle \varphi(0) \dots \varphi(n) \rangle)$ состоит, начиная с некоторого места, только из верных гипотез.

Пусть ε - действительное число, $0 < \varepsilon \leqslant 1$. Говорят, что F синтезирует класс U в смысле $GN(\varepsilon)$, если F - о.р.стратегия, и для любой $\varphi \in U$ в последовательности гипотез $F(\langle \varphi(0) \dots \varphi(n) \rangle)$ нижняя частота верных гипотез не меньше ε (см. [I]).

Если требование общерекурсивности стратегий ослабить до ч.р., то семейства синтезируемых классов GN, GN^{∞}, $GN(\varepsilon)$ не изменятся [I] .

Очевидно, $(1 > \varepsilon > \delta > 0)$:

$$GN \subseteq GN^{\infty} \subseteq GN(1) \subseteq GN(\varepsilon) \subseteq GN(\delta).$$

Уточнения:

а) Результат Я.М.Барздиня [2] : $GN \subset GN^{\infty}$

б) Результаты [I] : $\varepsilon > \frac{1}{2} \rightarrow GN(\varepsilon) = GN^{\infty}$,

$$GN^{\infty} \subset GN(\tfrac{1}{2}) \subset GN(\tfrac{1}{3}) \subset \cdots$$

Картину завершает

ТЕОРЕМА I. Если $q > 2$ -натуральное и $\frac{1}{q+1} < \varepsilon \leqslant \frac{1}{q}$, то $GN(\varepsilon) = GN(\frac{1}{q})$.

ДОКАЗАТЕЛЬСТВО. Пусть класс $U \in GN(\varepsilon)$ посредством о.р.стратегии F . Построим о.р.стратегию H , которая синтезирует любую $\varphi \in U$ с частотой верных гипотез не меньше $\frac{1}{q}$.

Пусть ε' -рациональное число, $\frac{1}{q+1} < \varepsilon' < \varepsilon$. Тогда, если $\varphi \in U$ и $h_i = F(<\varphi(0) \ldots \varphi(i)>)$, то для всех достаточно больших n среди чисел $(h_0 \ldots h_{n-1})$ будет более $\varepsilon' n$ геделевских номеров функции φ . Сначала построим алгоритм, перерабатывающий всякий набор гипотез $(g_0 \ldots g_{n-1})$ в некоторый набор из q гипотез $(a_1 \ldots a_q)$. Причем, если среди g_i более $\varepsilon' n$ геделевых номеров функции φ , то о д н а из a_j также должна быть геделевым номером φ .

Будем говорить, что набор $(g_0 \ldots g_{n-1})$ голосует за начальный кусок $y_0 y_1 \ldots y_t$, если для более чем $\varepsilon' n$ значений i гипотеза g_i обладает следующим свойством:

$$\varphi_{g_i}(0) = y_0 \wedge \varphi_{g_i}(1) = y_1 \wedge \ldots \wedge \varphi_{g_i}(t) = y_t .$$

Существует эффективная процедура P , перечисляющая всевозможные начальные куски, за которые голосует набор $(g_0 \ldots g_{n-1})$. Если среди g_i более $\varepsilon' n$ номеров функции φ , то в список, порождаемый процедурой P , войдут все начальные куски вида $\varphi(0)\ \varphi(1) \ldots \varphi(t)$. Кроме того, если считать эквивалентными куски, один из которых продолжает другой, то число классов эквивалентности в списке процедуры P не превышает q (это следует из неравенства $\varepsilon' > 1/q+1$). Каждый класс эквивалентности - это либо конечный кусок функции, либо полная функция.

Через a_1 обозначим геделев номер функции f_1 , вычисляемой следующим образом. Начальный кусок f_1 -первый кусок в списке процедуры P . Дальнейшие значения f_1 дают первое продолжение этого куска в списке P , и так далее. (Функция f_1 либо нигде не определена, либо всюду определена.)

Через a_2 обозначим геделев номер следующей функции φ_{f_2} . Начальный кусок f_2 - первый кусок в списке P , не являющийся начальным куском f_1 . Дальнейшие значения f_2 дает первое продолжение начального куска и т.д. (Функция f_2 может быть нигде не определенной даже если f_1 всюду определена.)

Аналогично f_3 отличается (если возможно) от f_1 и f_2 одновременно, и так далее. Получается набор из q гипотез $(a_1 \ldots a_q)$.

Легко убедиться (от противного), что любой кусок из списка процедуры P попадает в какую-либо из функций $f_1, \ldots, f_q$. Поэтому, если среди гипотез $(g_0 \ldots g_{n-1})$ более $\varepsilon' n$ геделевых номеров функции φ , то одна из функций f_i совпадает с φ , т.е. одна из гипотез набора $(a_1 \ldots a_q)$ будет геделевым номером φ .

Определим следующую о.р. стратегию H :

$$H(<\varphi(0) \ldots \varphi(qn+r)>) = a_{r+1},$$

где $n \geqslant 0$, $0 \leqslant r < q$ и $(a_1 \ldots a_q)$ - набор, полученный посредством построенного алгоритма из набора гипотез $(h_0 \ldots h_{n-1})$, где $h_i = F(<\varphi(0) \ldots \varphi(i)>)$. Если $\varphi \in U$, то для всех достаточно больших n среди q гипотез с порядковыми номерами

$$qn, \quad qn+1, \ldots, qn+q-1$$

одна будет верна, т.е. H синтезирует φ с частотой верных гипотез не меньше $1/q$.

Итак, $U \in GN(1/q)$. Теорема доказана.

ЗАМЕЧАНИЕ I. Конечные объединения классов из GN^∞ . Если $A_1, \ldots, A_k \in GN^\infty$, то как легко видеть, $A_1 \cup \ldots \cup A_k \in GN(1/k)$. В доказательстве теоремы 3 из [I] , по существу, построены k классов $B_i \in GN^\infty$ таких, что $B_1 \cup \ldots \cup B_k \notin GN(1/k-1)$. В качестве B_i там фигурирует класс таких о.р. функций φ , что $\varphi(i)$ - геделев номер ч.р. функции, совпадающей с φ , начиная с некоторого места. Таким образом, в терминах введенной иерархии полностью решен вопрос о сложности синтеза любых конечных объединений классов из GN^{∞}.

ПРОБЛЕМА. Сложность синтеза конечных объединений из GN. В [2] (теорема I) построены классы $A_1, A_2 \in GN$ такие, что $A_1 \cup A_2 \in GN(\frac{1}{2}) - GN^{\infty}$. Существуют ли классы $A_1, A_2, A_3 \in GN$ такие, что

$A_1 \cup A_2 \cup A_3 \in GN(\frac{1}{3}) - GN(\frac{1}{2})$?

2. Прогнозирование. По данным значениям $\varphi(0) \dots \varphi(n)$ требуется предсказать $\varphi(n+1)$. Если F - стратегия, а φ -функция, то значения $F(\langle \varphi(0) \dots \dots \varphi(n) \rangle)$ при $n = 0, 1, 2, \dots$ называют прогнозами. Прогноз верен, если он равен $\varphi(n+1)$, в противном случае его называют ошибкой.

Говорят, что F прогнозирует класс U в смысле NV, если F - о.р. стратегия, и для всех $\varphi \in U$ среди прогнозов F на φ не более чем конечное число ошибочных. Обозначим:

$$NV = \{U / \exists F \ (F \text{ прогнозирует } U \text{ в смысле } NV)\}$$

Ослабив требование общерекурсивности до ч.р., получаем понятие NV''. Добавляя в NV'' требование, чтобы при $\varphi \in U$ все прогнозы F на φ были определены, получаем понятие NV'. Обозначения семейств классов NV', NV'' понятны.

Очевидно: $NV \subseteq NV' \subseteq NV''$. Согласно [3] : $NV \subset NV'$, а в [I] показано, что $NV \subset GN$, $NV'' = GN^{\infty}$.

Пусть ε - действительное число, $0 < \varepsilon \leqslant 1$. Говорят, что F прогнозирует класс U в смысле $NV(\varepsilon)$, если F - о.р. стратегия, и для любой $\varphi \in U$ нижняя частота верных прогнозов F на φ не меньше ε. Аналогично определяются $NV'(\varepsilon)$ и $NV''(\varepsilon)$.

В [I] утверждается, что $(1 > \varepsilon > \delta > 0)$

$$NV \subset NV(1) \subset NV(\varepsilon) \subset NV(\delta),$$
$$NV' \subset NV'(1) \subset NV'(\varepsilon) \subset NV'(\delta).$$

В качестве класса, входящего в $NV(\delta)$, но не входящего в $NV'(\varepsilon)$, в [I] фигурирует

$U_\delta \{\varphi | \varphi \in R \wedge$ нижняя частота нулей в φ не меньше $\delta\}$.

Кроме того, $U_1 \in NV(1) - NV'$.

В случае $NV''(\varepsilon)$ ситуация совершенно противоположна: здесь $NV''(\varepsilon) = NV''(1)$ для всех $\varepsilon > 0$, как это показывает

ТЕОРЕМА 2. $R \in NV''(1)$, т.е. существует ч.р. стратегия, прогнозирующая с частотой 1 любую о.р. функцию.

ДОКАЗАТЕЛЬСТВО. Мы должны построить ч.р. стратегию F, которая на любой о.р. функции φ допускает ошибки с частотой 0. Пусть h - монотонная неограниченная о.р. функция такая, что $h(n) < n$ для всех n.

Для определения прогноза $F(<\varphi(0) \dots \varphi(n)>)$ берутся функции $\varphi_1, \varphi_2, \dots, \varphi_{h(n)}$ и среди них ищется φ_i такая, что

$$(\forall x \leq n)(\varphi_i(x) = \varphi(x) \wedge \varphi_i(n+1) \text{ определено}).$$

Если такое i найдено, полагаем:

$$F(<\varphi(0) \dots \varphi(n)>) = \varphi_i(n+1),$$

в противном случае прогноз неопределен.

Легко проверить, что стратегия F обладает следующими свойствами.

(а) Пусть φ - о.р. функция, и $n_0(\varphi)$ - наименьшее n такое, что $h(n)$ больше минимального геделева номера φ. Тогда при $n \geq n_0(\varphi)$ прогноз $F(<\varphi(0) \dots \varphi(n)>)$ определен.

(б) Для о.р.функции φ число ошибок среди первых n прогнозов стратегии F меньше $h(n)+n_0(\varphi)$.

Если в качестве h взять $h(n)=[\sqrt{n}]$, то получаемая ч.р.стратегия F на любой о.р.функции допускает ошибки с частотой 0.

Теорема 2 доказана.

Таким образом $P \subset NV''(1)$ для любого типа P (прогнозирования или синтеза), отличного от $NV''(\varepsilon)$.

Оставшиеся вопросы сравнения различных типов предельного синтеза и прогнозирования легко решаются с помощью двух следующих лемм. Это результаты двух видов: (а) устанавливается строгое включение двух типов, (б) устанавливается н е с р а в н и м о с т ь типов A, B, т.е. что соответствующие семейства $A-B$, $B-A$, $A\cap B$ все непусты. В доказательствах непустоты используются классы U_δ (особенно U_1, см. выше), а также два класса, построенные в доказательствах лемм I,2.

ЛЕММА I. Пусть $\mathcal{V}=\{i\varphi / \varphi\in R \wedge \varphi_i = i\varphi\}$. Тогда для всех $\varepsilon>0$, $\mathcal{V}\in NV'-NV(\varepsilon)$.

ДОКАЗАТЕЛЬСТВО. Класс $\mathcal{V}$ (введенный Я.М.Барздинем для доказательства включения $NV\subset NV'$) прогнозируем в смысле NV' следующей ч.р.стратегией F:

$$F(\langle \varphi(0)\dots\varphi(n)\rangle)=\varphi_{\varphi(0)}(n+1).$$

Покажем, что при $\varepsilon>0$: $\mathcal{V}\notin NV(\varepsilon)$. Пусть H - о.р.стратегия. Для каждого i легко построить о.р.функцию f_i такую, что на функции if_i H делает только ошибочные прогнозы. Теорема о неподвижной точке дает i_0 такое, что $i_0 f_{i_0}=\varphi_{i_0}$, т.е. $i_0 f_{i_0}\in\mathcal{V}$.

Лемма доказана.

ЛЕММА 2. Существует такой класс $W \in GN$, что $W \notin NV'(\varepsilon)$ для всех $\varepsilon > 0$.

ДОКАЗАТЕЛЬСТВО. Пусть $\{\kappa_m\}$ - рекурсивная возрастающая последовательность, частота которой в ряду всех натуральных чисел равна нулю. Искомый класс W состоит из всех о.р.функций φ, обладающих следующим свойством:

$$(\exists i)[\varphi_i = \varphi \wedge (\exists m_0\ \forall m > m_0)\ \varphi(\kappa_m) = i],$$

т.е.функция $\varphi \in W$, если некоторый ее геделев номер, определенным образом, встречается среди значений $\varphi(x)$.

Следующая о.р.стратегия F синтезирует класс W в смысле GN:

$$F(\langle \varphi(0) \dots \varphi(n) \rangle) = \begin{cases} 0 \text{ ; если } n < \kappa_0, \\ \varphi(\kappa_m) \text{ , если } \kappa_m \leq n < \kappa_{m+1}. \end{cases}$$

Покажем, что $W \notin NV'(\varepsilon)$ при $\varepsilon > 0$. С помощью теоремы о неподвижной точке легко показать, что в качестве начальных кусков функций класса W выступают произвольные кортежи натуральных чисел. Поэтому, если ч.р. стратегия H прогнозирует W в смысле $NV'(\varepsilon)$, все прогнозы H должны быть определены, т.е. H на самом деле - о.р.стратегия.

Воспользуемся этим. Для каждого i определяется о.р. функция

$$g_i(x) = \begin{cases} 0 \text{ , если } x = 0, \\ i \text{ , если } (\exists m)(x - \kappa_m > 0), \\ 1 + H(\langle g_i(0) \dots g_i(x-1) \rangle), \\ \qquad \text{в противном случае.} \end{cases}$$

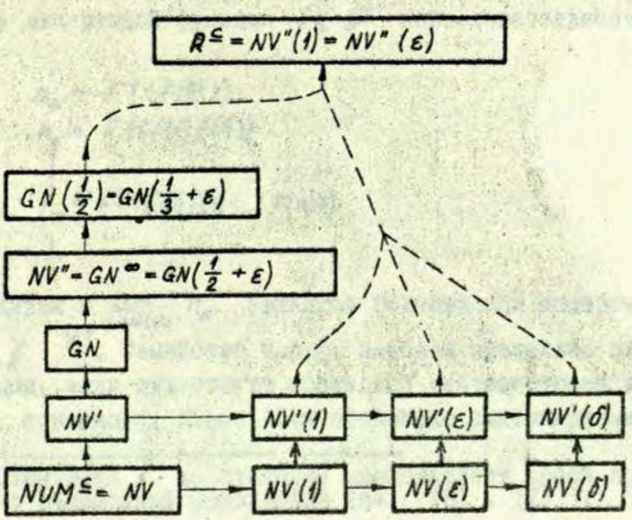
На всех g_i стратегия H делает ошибки с частотой 1 (ибо частота $\{\kappa_m\}$ равна 0). По теореме о неподвижной точке найдется i_1 такое, что $g_{i_1} = \varphi_{i_1}$, т.е. $g_{i_1} \in W$.

Лемма 2 доказана.

Используя приведенные результаты, сравнение различных типов предельного синтеза и прогнозирования можно довести до конца. Полученные результаты сводятся в следующую схему (построенную по образцу [4]). В этой схеме стрелка $\rightarrow$ означает строгое включение $\subsetneq$. Совпадающие понятия помещены в общую клетку. В случаях, когда из одной клетки в другую (и обратно) нет пути по стрелкам, доказано, что соответствующие типы несравнимы.

$NUM^{\subseteq}$ -семейство всех подклассов эффективно перечислимых классов о.р.функций, $R^{\subseteq}$ -семейство всех классов о.р.функций.

ПРИМЕР. Типы $NV(0,88)$; $NV'(0,93)$ несравнимы, т.е. (а), вообще говоря, нельзя повысить частоту верных прогнозов от $0,88$ до $0,93$ за счет перехода от о.р.стратегий к ч.р.стратегиям; (б), вообще говоря, нельзя получить о.р. стратегию вместо ч.р.стратегии, если разрешается понизить частоту верных прогнозов с $0,93$ до $0,88$.



$1 > \varepsilon > \delta > 0$

ЛИТЕРАТУРА

1. Подниекс К.М. Сравнение различных типов предельного синтеза и прогнозирования функций. - "Учен. зап. Латв. ун-та", 1974, т.210.
2. Бардинь Я.М. Две теоремы о предельном синтезе функций, там же.
3. Барздинь Я.М., Фрейвалд Р.В. Прогнозирование общерекурсивных функций. - ДАН СССР, 1972, т.206, № 3.
4. Klette R. Finitäre Erkennung allgemein-rekursiver Funktionen II, Sektion Mathematik der Friedrich - Schiller- Universität Jena, Jena, Juli 1974.

О СРАВНЕНИИ ПРЕДЕЛЬНОГО СИНТЕЗА И ПРЕДЕЛЬНОЙ СТАНДАРТИЗАЦИИ НОМЕРОВ ОБЩЕРЕКУРСИВНЫХ ФУНКЦИЙ

Е.Б.Кинбер

В настоящей статье рассматриваются следующие две задачи:

I. Предельный синтез. По последовательности значений общерекурсивной функции (о.р.ф.)

$$f(0),\ f(1),\ \dots,\ f(k),\ \dots$$

требуется в пределе найти ее геделевский номер. Более точно, пусть зафиксирована канторовская нумерация всех конечных кортежей натуральных чисел: $\langle a_1 a_2 \dots a_n \rangle$ — номер кортежа $(a_1, a_2, \dots, a_n)$. Будем говорить, что о.р.ф. F (называемая в дальнейшем стратегией) предельно синтезирует семейство о.р.ф. $\mathcal{F}$, если для каждой функции $f \in \mathcal{F}$ последовательность

$$\begin{aligned} n_0 &= F(\langle f(0) \rangle) \\ n_1 &= F(\langle f(0) f(1) \rangle) \\ &\vdots \\ n_k &= F(\langle f(0) f(1) \dots f(k) \rangle) \\ &\vdots \end{aligned} \qquad \text{(I)}$$

сходится и $\lim_{k \to \infty} n_k$ является геделевским номером функции f ж). Семейство о.р.ф. назовем предельно синтезируемым, если существует предельно синтезирующая его о.р. стратегия. Класс всех предельно синтезируемых се-

---

ж) Стратегия F по существу представляет собой предельно вычислимый функционал (см. [8], [7]).

мейств о.р.ф. обозначим, следуя [4] , через GN .

Задача предельного синтеза изучалась в работах [I] , [2] , [3] , [4] , [5] , [9] , а также в некоторых других.

В ряде работ (например, в [4] , [5] , [9]) изучалось несколько более слабое понятие предельного синтеза: требуется, чтобы в последовательности (I) начиная с некоторого k встречались только номера функции f (возможно, различные). Класс семейств о.р.ф., предельно синтезируемых в этом смысле, обозначим через GN^{∞} . Очевидно, $GN \subseteq GN^{\infty}$. В [5] доказано, что это включение строгое.

2. Предельная стандартизация. По произвольному номеру о.р.ф. f требуется в пределе найти ее некоторый фиксированный (стандартный) геделевский номер. Более точно, пусть зафиксирована геделевская нумерация всех о.р.ф. от одной переменной $\{\varphi_i\}_{i=0,1\ldots}$. Будем говорить, что семейство о.р.ф. $\mathcal{F}$ предельно стандартизируемо, если существует такая о.р.ф. $\psi(x,i)$, что для любой о.р.ф. $f \in \mathcal{F}$ и ее различных номеров n и m :

а) $\lim\limits_{i} \psi(n,i)$ и $\lim\limits_{i} \psi(m,i)$ существуют

б) $\lim\limits_{i} \psi(n,i) = \lim\limits_{i} \psi(m,i) = k$

в) $\varphi_k = f$ (k - "стандартный" номер).

Функция ψ представляет собой предельно эффективную операцию [7] (аналогичную обычным эффективным операциям [8]).

Заметим, что понятие предельной стандартизации инвариантно относительно геделевских нумераций: если семейство о.р.ф. предельно стандартизируемо в одной геделевской нумерации, то оно предельно стандартизируемо и в любой другой.

Класс всех предельно стандартизируемых семейств о.р.ф. обозначим через LS. Очевидно, $GN \subseteq LS$. Я.М.Барздинем был поставлен вопрос о том, совпадают ли эти классы. Из доказываемой ниже теоремы I следует, что класс LS шире класса GN. Заметим, что отличие класса в с е х предельно вычислимых функционалов (а не только стратегий) от класса предельно эффективных операций на множестве всех о.р.ф. было доказано в [7].

ТЕОРЕМА I. $LS \setminus GN^{\infty} \neq \varnothing$.

Прежде чем доказывать теорему, введем некоторые обозначения.

Для любых кортежей натуральных чисел $\bar{\alpha}$ и $\bar{\beta}$ через $\bar{\alpha}\bar{\beta}$ условимся обозначать кортеж, состоящий из элементов $\bar{\alpha}$ и следующих за ними элементов $\bar{\beta}$. Если $\bar{\beta}$ содержит только одно число (например, i), то вместо $\bar{\alpha}\bar{\beta}$ будем пользоваться обозначением $\bar{\alpha}i$. Аналогично определяется кортеж $i\bar{\alpha}$. Длину произвольного кортежа $\bar{\alpha}$ обозначим через $\ell(\bar{\alpha})$.

Произвольную функцию f мы будем отождествлять с последовательностью ее значений; в этом случае для функций, почти всюду равных нулю, удобно использовать обозначения типа $i0^{\infty}$, $\bar{\alpha}i0^{\infty}$, $\bar{\alpha}\bar{\beta}0^{\infty}$ ($\bar{\alpha} = (a_1, a_2, \ldots, a_n)$ и $\bar{\beta} = (b_1, b_2, \ldots, b_m)$ - кортежи натуральных чисел) и т.п. Так, например, $\bar{\alpha}i0^{\infty}$ - функция, которая на $x \leqslant n-1$ равна a_x, на $x=n$ равна i, а в остальных точках - нулю.

Наконец, для любой функции f, определенной на всех $x \leqslant k$, через $f^{[k]}$ условимся обозначать кортеж $(f(0), f(1), \ldots, f(k))$.

ОПРЕДЕЛЕНИЕ. Назовем семейство о.р.ф. $\mathcal{F}$ всюду плотным, если для любого кортежа натуральных чисел $\bar{\alpha} = (a_0, a_1, \ldots, a_n)$ существует такая функция $f \in \mathcal{F}$, что $f^{[n]} = \bar{\alpha}$ ($\mathcal{F}$, очевидно, всюду плотно в бэровской метрике на N^N).

Зафиксируем произвольную геделевскую нумерацию $A=\{\varphi_i\}_{i=0,1,\dots}$ всех частично-рекурсивных функций (ч.р.ф.). Обозначим через O_A семейство о.р.ф. f для которых $\varphi_{f(0)}=f$.

ЛЕММА I. Пусть $\mathcal{F}$ - произвольное всюду плотное семейство о.р.ф. Тогда $\mathcal{F}\cup O_A\notin GN^{\infty}$.

ДОКАЗАТЕЛЬСТВО по существу представляет собой несколько более сложный вариант доказательства теоремы I из [5], но для полноты изложения мы приведем его. Предположим, от противного, что семейство $\mathcal{F}\cup O_A$ предельно синтезирует (в смысле GN^{∞}) некоторая о.р.стратегия H.

Поскольку $\mathcal{F}\cup O_A$ всюду плотно и H предельно синтезирует $\mathcal{F}\cup O_A$, то по любому кортежу $\bar{\alpha}$ можно эффективно найти такой кортеж $\bar{\beta}$, что функция φ_r с номером $r=H(\bar{\alpha}\bar{\beta})$ определена на $\ell(\bar{\alpha}\bar{\beta})$.

Пользуясь этим обстоятельством, определим для любого i о.р.ф. $\varphi_{g(i)}$. Полагаем $\varphi_{g(i)}(0)=i$. Затем находим такой $\bar{\beta}_1$, что функция φ_{r_1} с номером $r_1=H(i\bar{\beta}_1)$ определена на $k_1=\ell(i\bar{\beta}_1)$, и полагаем $\varphi_{g(i)}^{[k_1-1]}=i\bar{\beta}_1$ и $\varphi_{g(i)}(k_1)=\varphi_{r_1}(k_1)+1$. Далее находим такой $\bar{\beta}_2$, что φ_{r_2} с номером $r_2=H(\varphi_{g(i)}^{[k_1]}\bar{\beta}_2)$ определена на $k_2=\ell(\varphi_{g(i)}^{[k_1]}\bar{\beta}_2)$, и полагаем $\varphi_{g(i)}^{[k_2-1]}=\varphi_{g(i)}^{[k_1]}\bar{\beta}_2$ и $\varphi_{g(i)}(k_2)=\varphi_{r_2}(k_2)+1$ и т.д. Функции $g(i)$ и $\varphi_{g(i)}$ при любом i, очевидно, о.р.ф. По теореме о неподвижной точке существует такое a, что $\varphi_a=\varphi_{g(a)}$, т.е. $\varphi_a(0)=a$. Следовательно, $\varphi_a\in O_A$. Но стратегия H на φ_a бесконечно много раз выдает числа, не являющиеся номерами φ_a, и поэтому не может предельно синтезировать φ_a. Лемма I доказана.

Теперь мы построим такое всюду плотное семейство о.р.ф. $\mathcal{F}$, что $\mathcal{F}\cup O_A\in LS$.

Введем понятие минимальной программы для кортежа $\bar{\alpha} = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n)$ в геделевской нумерации A :

$$\kappa_A(\bar{\alpha}) = \min\left\{p \mid \forall i \leq n\,(\varphi_p(i) = \varepsilon_i)\right\}.$$

Далее пусть для любой о.р.ф. f

$$d_A(f) = \operatorname{card}\left\{r \mid \kappa_A(f^{[r]}) > r\right\}.$$

Обозначим минимальный номер о.р.ф. f в A через $m_A(f)$. Очевидно, $d_A(f) < m_A(f)$.

Рассмотрим следующее семейство о.р.ф. :

$$\mathcal{F}_A = \left\{f \mid m_A(f) < d_A^2(f) \text{ и } f \text{ - о.р.ф.}\right\}.$$

Очевидно, для разных нумераций A семейства $\mathcal{F}_A$, вообще говоря, различны.

ЛЕММА 2. Существует такая геделевская нумерация всех ч.р.ф. $\tilde{A}$, что $\mathcal{F}_{\tilde{A}}$ - всюду плотное семейство о.р.ф.

ДОКАЗАТЕЛЬСТВО. Нумерацию $\tilde{A}$ мы определим, исходя из произвольной фиксированной геделевской нумерации $A = \left\{\varphi_i\right\}_{i=0,1\ldots}$. Условимся обозначать i - ую функцию в $\tilde{A}$ через $\tilde{\varphi}_i$.

Зафиксируем эффективную нумерацию P всех кортежей натуральных чисел, в которой длина кортежа не превосходит его номера.

Полагаем для $i < 4$ $\tilde{\varphi}_i = \varphi_0$ и для каждого $\kappa \geq 1$ $\tilde{\varphi}_{2^\kappa} = \varphi_\kappa$. Далее пусть $\bar{\alpha}$ - кортеж, имеющий в P номер κ . Для всех i , где $2^{2^\kappa} < i < 2^{2^{\kappa+1}}$, полагаем $\tilde{\varphi}_i = \bar{\alpha}\, i\, 0^\infty$. Определение $\tilde{A}$ завершено. Очевидно, $\tilde{A}$ - геделевская нумерация всех ч.р.ф.

Покажем, что семейство $\mathcal{F}_{\tilde{A}}$ - всюду плотно. Пусть $\bar{\alpha}$ - произвольный кортеж (имеющий в P номер κ). Достаточно показать, что одна из функций $\bar{\alpha}\, i\, 0^\infty$, где $2^{2^\kappa} < i < 2^{2^{\kappa+1}}$, принадлежит $\mathcal{F}_{\tilde{A}}$.

Число различных $\widetilde{\varphi}_j$ с номерами $j < 2^{2^k}$ не превосходит 2^{2^k}. Поэтому по крайней мере для одного i_0, где $2^{2^{k+1}} - (2^{2^k}+2) \leq i_0 < 2^{2^{k+1}}$,

$$k_{\widetilde{A}}(\bar{\alpha}\, i_0) > 2^{2^k}.$$

Но в таком случае в силу определения $\widetilde{A}$

$$k_{\widetilde{A}}(\bar{\alpha}\, i_0) = m_{\widetilde{A}}(\bar{\alpha}\, i_0\, 0^\infty) \geq 2^{2^{k+1}} - (2^{2^k}+2) \quad (2)$$

Пусть $f = \bar{\alpha}\, i_0\, 0^\infty$. Из (2) следует, что для всех $r \geq \ell(\bar{\alpha}\, i_0) = k+1$

$$k_{\widetilde{A}}(f^{[r]}) = m_{\widetilde{A}}(f).$$

Таким образом, для всех r, где $k+1 \leq r < 2^{2^{k+1}} - (2^{2^k}+2)$,

$$k_{\widetilde{A}}(f^{[r]}) > r,$$

т.е. $d_{\widetilde{A}}(f) \geq 2^{2^{k+1}} - (2^{2^k}+2) - (k+1) - 1$. Так как $m_{\widetilde{A}}(f)$, очевидно, не превосходит $2^{2^{k+1}}$, то при любом достаточно большом k должно выполняться неравенство

$$m_{\widetilde{A}}(f) < d^2_{\widetilde{A}}(f).$$

Итак, если $\bar{\alpha}$ имеет достаточно большую длину, то $\bar{\alpha}\, i_0\, 0^\infty \in \mathcal{F}_{\widetilde{A}}$. Лемма 2 доказана.

Из лемм I и 2 следует

ЛЕММА 3. $\mathcal{F}_{\widetilde{A}} \cup \mathcal{O}_{\widetilde{A}} \notin GN^\infty$.

Покажем теперь, что семейство $\mathcal{F}_{\widetilde{A}} \cup \mathcal{O}_{\widetilde{A}}$ предельно стандартизируемо.

ЛЕММА 4 (Я.М.Барздинь). Если для семейства о.р.ф. существует такая ч.р.ф. $\nu(x)$, что

(*) $\forall f \in \mathcal{F} [\varphi_k = \varphi_n = f \Rightarrow (\nu(k) = \nu(n) \,\&\, m_A(f) < \nu(n))]$,

то $\mathcal{F} \in LS$.

ДОКАЗАТЕЛЬСТВО. Нам необходимо определить предельно эффективную операцию $\psi(x,j)$, предельно стандартизирующую $\mathcal{F}$.

Пусть $f \in \mathcal{F}$, $\varphi_n = f$ и $\nu(n) = r$. Будем постепенно сравнивать функцию φ_n с каждой из функций φ_i, $i < r$ (ведя необходимые вычисления по тактам); как только выяснится, что $\varphi_i \neq \varphi_n$, номер i зачеркиваем. Пусть j – произвольный шаг описанной процедуры. Полагаем $\psi(n,j) = k$, где k – некоторый фиксированный номер функции g, вычисляемой в соответствии со следующими инструкциями:

"для вычисления $g(x)$ нужно параллельно вычислять $\varphi_{i_1}(x), \varphi_{i_2}(x), \ldots, \varphi_{i_s}(x)$, где $i_1, i_2, \ldots, i_s$ – незачеркнутые к этому моменту номера $< r$; как только одно из значений $\varphi_{i_p}(x)$ будет определено, нужно положить $g(x) = \varphi_{i_p}(x)$."

Со временем номера всех функций φ_i, $i < r$, для которых $\exists x (\varphi_i(x)$ определено $\& \varphi_i(x) \neq f(x))$, будут зачеркнуты. С другой стороны, среди функций с номерами $i < r$ присутствует f. Отсюда легко следует, что начиная с некоторого j_0 для всех $j > j_0$ $\psi(n,j)$ будет одним и тем же номером f. Лемма 4 доказана.

ЗАМЕЧАНИЕ I. Незначительное изменение доказательства показывает, что для справедливости леммы 4 достаточна предельная вычислимость $\nu(x)$; т.е. $\nu(x) = \lim_i \nu'(x,i)$, где $\nu'(x,i)$ – о.р.ф. такая, что для любой $\varphi_n \in \mathcal{F}$ $\lim_i \nu'(n,i)$ определен.

ЛЕММА 5. Для класса $\mathcal{F}_{\bar{A}} \cup O_{\bar{A}}$ существует предельно вычислимая функция $\nu(x)$, удовлетворяющая условию (*).

ДОКАЗАТЕЛЬСТВО. Покажем, что в качестве $\nu(x)$ можно взять

$$\nu(x) = \max(d^2_{\bar{A}}(\varphi_x), \varphi_x(0)).$$

Из определения $\mathcal{F}_{\bar{A}}$ и $O_{\bar{A}}$ следует, что для любой о.р.ф. $\varphi_n \in \mathcal{F}_{\bar{A}} \cup O_{\bar{A}}$ $m_{\bar{A}}(\varphi_n) < \nu(n)$. Нужно показать, что $\nu(x)$ предельно вычислима. Для этого достаточно, очевидно, убедиться в том, что предельно вычислимой является функция $\mu(x) = d_{\bar{A}}(\varphi_x)$.

Пусть $\varphi_n \in \mathcal{F}_{\bar{A}} \cup O_{\bar{A}}$. Тогда, очевидно, $d_{\bar{A}}(\varphi_n) < n$ и для каждого i $\kappa_{\bar{A}}(\varphi_n^{[i]}) < n$. Используя последнее обстоятельство, нетрудно построить такую о.р.ф. $u(i,\kappa)$, что $\forall i < n$ $\kappa_{\bar{A}}(\varphi_n^{[i]}) = \lim\limits_{\kappa} u(i,\kappa)$. Следовательно, можно в пределе эффективно найти и число таких i, что $\kappa_{\bar{A}}(\varphi_n^{[i]}) > i$, т.е. $d_{\bar{A}}(\varphi_n)$.
Указанную процедуру можно осуществить, очевидно, и для любой ч.р.ф. $\varphi_n \in \mathcal{F}_{\bar{A}} \cup O_{\bar{A}}$ (результат процедуры в этом случае нас не интересует). Лемма 5 доказана.

Непосредственно из леммы 4 и 5 и замечания I следует

ЛЕММА 6. $\mathcal{F}_{\bar{A}} \cup O_{\bar{A}} \in LS$.

Теорема I следует из леммы 3 и 6.

Как уже отмечалось выше, любое семейство о.р.ф. из GN предельно стандартизируемо. Но уже в GN^* существуют семейства о.р.ф., которые не содержатся в LS.

ТЕОРЕМА 2. $GN^* \setminus LS \neq \emptyset$.

ДОКАЗАТЕЛЬСТВО. Пусть $\{\psi_i(x,\kappa)\}_{i=0,1\dots}$ - геделевская нумерация всех ч.р.ф. от двух переменных. По каждой $\psi_i(x,\kappa)$ можно эффективно найти такую о.р.ф. $\psi_{h(i)}(x,\kappa)$, что

$$\forall x\,(\lim_{\kappa}\psi_{h(i)}(x,\kappa)=\lim_{\kappa}\psi_i(x,\kappa)).$$

В дальнейшем нас будут интересовать числа типа $\lim\psi_i(x,\kappa)$, поэтому ниже через $\psi_i(x,\kappa)$ мы будем обозначать функцию $\psi_{h(i)}(x,\kappa)$. Зафиксируем также геделевскую нумерацию всех ч.р.ф. от одной переменной $\{\varphi_i\}_{i=0,1\dots}$.

Для каждой пары чисел (i,j) определим функцию $\varphi_{g_i(j)}$, вычисляемую в соответствии со следующими инструкциями.

Полагаем $\varphi_{g_i(j)}(0)=i$ и $\varphi_{g_i(j)}(1)=j$.

Далее для вычисления $\varphi_{g_i(j)}$ мы будем использовать определяемую ниже процедуру, имеющую два параметра u и n.

Пусть n - некоторый фиксированный геделевский номер функции $\lambda 0^{\infty}$. Полагаем $u=2$ и переходим к основной процедуре.

Основная процедура.

Этап 1. Если $\psi_i(n,u)=\psi_i(j,u)$, то переходим к этапу 2. Если $\psi_i(n,u)\neq\psi_i(j,u)$, то полагаем $\varphi_{g_i(j)}(u)=0$ и переходим к началу основной процедуры, используя в качестве u число $u+1$.

Этап 2. Начинаем вычислять $\varphi_{a_u}(u)$, полагая на r-ом $(r\geqslant 0)$ такте вычислений $\varphi_{g_i(j)}(u+r+1)=0$. Параллельно вычисляем две последовательности

$$a_{u+r}=\psi_i(n,u+r),\quad r=0,1,\dots$$

$$b_{u+r}=\psi_i(j,u+r),\quad r=0,1,\dots$$

Все три процесса продолжаются до тех пор, пока на некотором шаге r' не наступит одно из следующих событий:

А. Вычисление $\varphi_{a_u}(u)$ заканчивается и $\varphi_{a_u}(u) \neq 0$

Б. Вычисление $\varphi_{a_u}(u)$ заканчивается и $\varphi_{a_u}(u) = 0$

В. $a_{u+r'} \neq b_{u+r'}$

Г. $a_{u+r'} = b_{u+r'}$, но $a_{u+r'} \neq a_u$.

Определение основной процедуры завершено.

Если ни одно из перечисленных событий не наступит, то $\varphi_{g_i(j)}$ в точке u не будет определена.

Если первым наступит событие A , то полагаем $\varphi_{g_i(j)}(u) = 0$ и продолжаем вычислять a_{u+r} и b_{u+r} и определять $\varphi_{g_i(j)}(u+r+1)$, ожидая наступления события В или Г.

Если первым наступит событие Б, то полагаем $\varphi_{g_i(j)} = 1$ и переходим к основной процедуре, взяв в качестве параметра u число $u+r'+1$ и в качестве n - какой-нибудь геделевский номер функции $\bar{\alpha}\, 0^\infty$, где $\bar{\alpha} - \varphi_{g_i(j)}^{[u+r']}$

Если наступит событие В или Г., то переходим к основной процедуре, используя в качестве u число $u+r'+1$; параметр n при этом не меняется.

Нетрудно убедится, что для каждого i функция g_i - о.р.ф. и при любых i и j $\varphi_{g_i(j)}$ - либо о.р.ф., либо ч.р.ф., не определенная лишь в одной точке.

Для каждой функции $\varphi_{g_i(j)}$ полагаем

$$\varphi_{i_j}(x) = \begin{cases} \varphi_{g_i(j)}(x), & \text{если } \varphi_{g_i(j)}(x) \text{ определено} \\ 0 & \text{, в противном случае.} \end{cases}$$

Обозначим через $\mathcal{F}$ семейство о.р.ф. $\{\varphi_{i_j}\}$, $i = 0,1, \ldots, j = 0,1, \ldots$

Покажем, что $\mathcal{F} \notin LS$. Допустим от противного, что $\mathcal{F} \in LS$ и ψ_i - фунция, осуществляющая предельную стандартизацию для $\mathcal{F}$.

Заметим, что каждая из функций $\varphi_{g_i(j)}$ $(j=0,1,\dots)$ - о.р.ф. В самом деле, предположим, что $\varphi_{g_i(j)}$ не определена в точке u. Нетрудно убедиться, что $\varphi_{i,j}$ имеет вид $\bar{\alpha}\,0^\infty$, где $\bar{\alpha}$ - набор значений $\varphi_{g_i(j)}$ на $x<u$, причем основная процедура, начиная с некоторого момента, применяется к геделевскому номеру n функции $\bar{\alpha}\,0^\infty$.
Так как $\bar{\alpha}\,0^\infty \in \mathcal{F}$ и ψ_i предельно стандартизирует $\mathcal{F}$, то на некотором шаге основной процедуры, примененой к u и n, обязательно должно произойти событие Б. Следовательно, $\varphi_{g_i(j)}$ будет определена и в точке u -противоречие.

Применим к функции $g=g_i$ теорему о неподвижной точке; пусть $\varphi_{g(m)}=\varphi_m$. Так как $\varphi_{g(m)}$ - о.р.ф., то основная процедура при каждом ее применении должна приводить к одному из событий.А,Б,В или Г. В таком случае одно из этих событий должно происходить бесконечно много раз. Так как $\lim\limits_k \psi_i(m,k)$ существует и $\lim\limits_k \psi_i(m,k)=$ $=\lim\limits_k \psi_i(g(m),k)$, то события В и Г могут происходить, очевидно, лишь конечное число раз. Пусть $\lim\limits_k \psi_i(m,k)=c_m$. В силу определения предельной стандартизации c_m является номером для φ_m, поэтому событие А также может повториться лишь конечное число раз. Но если бесконечно много раз происходит событие Б, то в последовательности $\psi_i(m,0),\ \psi_i(m,1),\dots$ бесконечно много элементов не являются номерами φ_m. Итак, $\mathcal{F}\notin LS$.

Покажем теперь, что $\mathcal{F}\in GN^\infty$. Нам необходимо определить о.р.стратегию H, предельно синтезирующую $\mathcal{F}$ (в смысле GN^∞).

Пусть f - произвольная всюду определенная функция. Мы полагаем $H(\langle f(0)\rangle)=H(\langle f(0)f(1)\rangle)=0$ и для всех $k\geq 2$

$$H(\langle f(0)f(1)\dots f(k)\rangle)=n_k\,,$$

где n_k - геделевский номер следующей функции:

$$g(x) = \begin{cases} f(x) & \text{, если } x \leq k \\ \varphi_{g_i(j)}(x) & \text{, если } x > k \end{cases} \text{ ;здесь } i = f(0) \text{ и } j = f(1)$$

Легко убедиться,что для любой функции $f = \varphi_{i,j} \in \mathcal{F}$, начиная с некоторого k, все n_k будут номерами f. Стратегия H, очевидно,общерекурсивна. Таким образом, $\mathcal{F} \in GN^{\infty}$. Теорема 2 доказана.

ЛИТЕРАТУРА

I. Gold E.M.Languaqe identification in the limit.-"Information and control", 1967, v.10, No.5.
2. Барздинь Я.М.,Фрейвалд Р.В.Прогнозирование общерекурсивных функций.-ДАН СССР,I972,т.206, № 3.
3. Барздинь Я.М.,Подниекс К.М. К теории индуктивного вывода.-Труды симпозиума "Mathematical foundations of computer science",High Tatras, Czechoslovakia, 1973.
4. Подниекс К.М.Сравнение различных типов предельного синтеза и прогнозирование функций.-"Учен.зап.Латв.ун-та", I974,т.2IO.
5. Барздинь Я.М.Две теоремы о предельном синтезе.-"Учен. зап.Латв.ун-та",I974,т.2IO.
6. Blum L., Blum M. Towards a mathematical theory of inductive inference.-Preprint.
7. Барздинь Я.М.Об одном свойстве предельно вычислимых функционалов.-"Уч.зап.Латв.ун-та",I974,т.2IO.
8. Роджерс X.Теория рекурсивных функций и эффективная вычислимость, М., I972.
9. Feldman J.Some decidability results on grammatical inference and complexity.-"Information and control", 1972,v.20, No.3.

ВЕРОЯТНОСТНОЕ ПРОГНОЗИРОВАНИЕ ВЫЧИСЛИМЫХ ФУНКЦИЙ

К.М.Подниекс

§ I. Аппарат

Прогнозирование - это предсказывание значения $\varphi(m+1)$ по данным значениям $\varphi(0) \ldots \varphi(m)$ (здесь φ - всюду определенные функции типа $N \to N$). Прогноз вероятностной стратегии (или, короче, В-стратегии) представляет собой случайную величину, в частности, он будет верным с некоторой вероятностью.

Более точно, В-стратегия M задается:

(I) некоторым вероятностным пространством (Ω, B, P), где Ω - множество элементарных событий, B -борелевское поле событий, для которых определена вероятностная мера P;

(2) некоторым отображением M типа $N^* \to Z$, где N^* - множество всех конечных кортежей натуральных чисел (включая пустой кортеж), Z - множество всех случайных величин над пространством (Ω, B, P), принимающих значения в $N \cup \{\infty\}$. Заметим, что здесь <u>не</u> требуется, чтобы случайные величины, соответствующие различным кортежам, были независимы.

Для В-стратегии M и функции φ мы будем через $M(\varphi, m)$, где $m = 0, 1, \ldots$, обозначать случайные величины $M(\varphi(0) \ldots \varphi(m))$, т.е. прогнозы стратегии M на функции φ. Кроме того, $M(\varphi, -1)$ означает $M(\Lambda)$, где Λ - пустой кортеж.

Особый интерес представляет вероятность

$$P_m\{M, \varphi\} = P\{M(\varphi, m) \neq \varphi(m+1)\},$$

т.е. вероятность того, что прогноз $M(\varphi, m)$ будет ошибкой.

На пространстве (Ω, B, P) определены также вероятности

$$P\{M,\varphi,=k\}, \quad P\{M,\varphi,\leq k\}$$

того, что M сделает на φ точно k (не более k) ошибок. В самом деле, соответствующие события можно выразить через события вида $\{M(\varphi,m)=\varphi(m+1)\}$, используя только операции дополнения и счетного объединения. Например:

$$\{M,\varphi,=0\}=\bigcap_{m\in N}\{M(\varphi,m)=\varphi(m+1)\},$$

$$\{M,\varphi,=1\}=\bigcup_{n\in N}\Big[\{M(\varphi,n)\neq\varphi(n+1)\}\cap\bigcap_{\substack{m\in N\\ m\neq n}}\{M(\varphi,m)=\varphi(m+1)\}\Big]$$

По аналогии со случаем детерминированных стратегий [I] , где считается, что стратегия прогнозирует функцию φ , если она допускает на φ не более чем конечное число ошибок, будем говорить, что В-стратегия M п р о г н о з и р у е т функцию φ , если M допускает на φ с вероятностью 1 не более чем конечное число ошибок, т.е. если

$$\sum_{k=0}^{\infty} P\{M,\varphi,=k\}=1$$

ЛЕММА I. Если сумма вероятностей ошибок $\sum_m P_m\{M,\varphi\}<\infty$, то В-стратегия M прогнозирует функцию φ . Если же эта сумма $=\infty$ и прогнозы M на φ независимы, то $P\{M,\varphi,=k\}=0$ для всех k .

ДОКАЗАТЕЛЬСТВО. Непосредственно, с помощью леммы Бореля-Кантелли [2] .

Среди всех В-стратегий практически интересны, конечно, только те, которые можно как-то реализовать на (специальных) машинах Тьюринга. Эти т.н. в е р о я т -

ностные машины впервые рассматривали Де Леу, Мур и др. в [3] , для предельного синтеза они использовались Я.М.Барздинем [4] .

Рассмотрим следующую четырехленточную машину Тьюринга $\mathfrak{M}$ (число лент здесь несущественно). Первая лента-рабочая. На второй ленте записана произвольная бесконечная 01 -последовательность. На этой ленте $\mathfrak{M}$ имеет одну только-читающую головку, которая все время двигается вправо. На третьей ленте записана последовательность значений:

$$\varphi(0), \quad \varphi(1), \ \ldots, \ \varphi(m), \ldots$$

функции φ , которую $\mathfrak{M}$ должна прогнозировать. На этой ленте $\mathfrak{M}$ имеет одну только-читающую головку (без ограничений движения). Четвертая лента вначале пуста, на ней $\mathfrak{M}$ имеет одну только-пишущую головку, которая может стоять на месте либо двигаться вправо (но не может двигаться влево).

Если машину $\mathfrak{M}$ в такой ситуации запустить, она должна вычислить и печатать на четвертой ленте пустую, конечную или бесконечную последовательность:

$$a_{-1}, a_0, a_1, \ldots, a_m, \ldots$$

причем для вычисления a_m ей разрешается использовать только значения $\varphi(0) \ldots \varphi(m)$.

Запись на второй ленте мы будем интерпретировать как результат работы бернуллиевского датчика нулей и единиц (распределение $p = q = \frac{1}{2}$). Точнее это значит, что на основе множества Ω_0 всех бесконечных 01 - последовательностей вводится следующее вероятностное пространство (Ω_0, B_0, P_0) . Здесь B_0 - наименьшее борелевское поле, содержащее все множества вида

$$\Omega_{\bar{\alpha}} = \{\omega \in \Omega_0 / \omega_0 = \alpha_0 \wedge \ldots \wedge \omega_{n-1} = \alpha_{n-1}\},$$

где $\bar{\alpha}=\alpha_0\alpha_1\ldots\alpha_{n-1}$ - произвольное двоичное слово. Если определить $\mu(\Omega_{\bar{\alpha}})=2^{-n}$, то интересующая нас мера P_0 будет (единственным) продолжением μ на все поле B_0 (см. [2]).

На пространстве (Ω_0, B_0, P_0) легко определить вероятности событий вида "машина $\mathfrak{M}$ по данным $\varphi(0)\ldots\varphi(m)$ печатает a_m, равное числу t " или "для данных $\varphi(0)\ldots\varphi(m)$ значение a_m неопределено". Таким образом, машина $\mathfrak{M}$, по существу, реализует некоторое отображение из множества N^* всех конечных кортежей натуральных чисел в множество случайных величин над пространством (Ω_0, B_0, P_0), принимающих значения в $N\cup\{\infty\}$ (кортежу $\varphi(0)\ldots\varphi(m)$ соответствует случайная величина a_m). Машина $\mathfrak{M}$ реализует, таким образом, некоторую В-стратегию.

В-стратегии, порожденные машинами указанного типа, будем называть р е к у р с и в н ы м и В - с т р а т е г и я м и.

Это определение рекурсивных В-стратегий допускает неограниченно долгое вычисление отдельного прогноза. Например, прогноз a_{-1} может быть равен t с вероятностью 2^{-t}, и это - для всех $t>1$. Выделим особо В-стратегии, лишенные этого недостатка.

Пусть U - класс функций. Будем говорить, что В-стратегия M ф и н и т н а н а U, если для любой $\varphi\in U$ и любого набора $(n_{-1}, n_0\ldots n_{m-1})\in N^*$ (в случае $m=-1$ берется пустой набор) при условии $(\forall_i<m)\ M(\varphi,i)=n_i$ (для $m=-1$ это условие выполняется с вероятностью 1):

(а) найдется конечное множество натуральных чисел A такое, что $M(\varphi,m)\in A$ с вероятностью 1,

(б) для всех $t\in A$ вероятность события $M(\varphi,m)=t$ является двоично рациональным числом (т.е. числом вида $a2^{-b}$, где $a,b\in N$).

Используя бернуллиевский датчик распределения $(\frac{1}{2}\frac{1}{2})$, каждое финитное распределение вероятностей можно реализовать за ограниченное время.

В-стратегия называется всюду финитной, если она финитна на классе всех о.р.функций.

§ 2. Результаты

В этой статье изучаются оценки числа ошибок, допускаемых В-стратегиями при прогнозировании нумерованных классов (U, τ) (где U -эффективно перечислимый класс о.р.функций, τ -некоторая вычислимая его нумерация). Что в этом случае понимать под оценкой? Если В-стратегия M прогнозирует все функции класса U и при этом

$$P\{M, \tau_n, \leq f(n)\} \to 1$$

когда $n \to \infty$, то имеет смысл говорить, что M допускает на τ_n, как правило, не более $f(n)$ ошибок. Функции типа $f(n)$ и будем считать оценками числа ошибок при вероятностном прогнозировании нумерованного класса (U, τ)

Целью этой статьи является доказательство того, что функцию $f(n)$ можно выбрать асимптотически равной $\frac{1}{2}\log_2 n$, но не лучше. Начнем с нижней оценки.

ТЕОРЕМА I. Существует нумерованный класс (U, τ) такой, что для любой В-стратегии M :

$$(\exists^\infty_n)\ P\{M, \tau_n, \geq \tfrac{1}{2}\log_2 n\} > \tfrac{1}{2}.$$

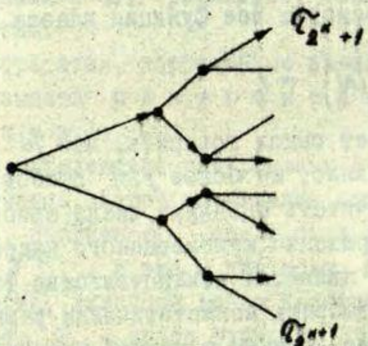
ДОКАЗАТЕЛЬСТВО. Нумерация τ строится в виде эффективно растущей двумерной таблицы значений $\tau_n(x)$:

$$T_1 = \boxed{\begin{array}{c}0\\ \hline 1\end{array}}\,, \qquad T_{k+1} = \begin{array}{|c|c|}\hline T_k & \begin{array}{c}0\\0\\ \vdots\\0\end{array}\\ \hline T_k & \begin{array}{c}1\\1\\ \vdots\\1\end{array}\\ \hline\end{array}$$

Очевидно, получился класс:

$$U = \left\{ \bar{\alpha}\ 0^{\infty} \ \middle|\ \bar{\alpha} \text{ - двоичное слово} \right\}.$$

Кроме того, таблица T_k содержит в точности все 2^k двоичных слова длины k. Поэтому дерево функций τ_n, где $2^k < n \le 2^{k+1}$, является полным двоичным деревом высоты k, например, для $k=3$:



Пусть В-стратегия M определена на пространстве (Ω, B, P). Каждому элементарному событию $\omega \in \Omega$ однозначно соответствует некоторый набор прогнозов в отмеченных 2^k-1 вершинах указанного дерева, на чертеже эти прогнозы обозначены стрелками. Стрелки можно расставить 2^{2^k-1} способами. Через A_i обозначим события, соответствующие расстановкам $(i=1,2,\ldots,2^{2^k-1})$.

Вероятность того, что среди первых k прогнозов стратегии M на функции $\tau_n\ (2^k<n\le 2^{k+1})$ будет точно j ошибок, выражается суммой некоторых $P(A_i)$. Под-

считаем число этих слагаемых. Из k вершин, через которые проходит τ_n, в j вершинах стрелки должны уходить в сторону от τ_n. В тех 2^k-1-k вершинах, через которые τ_n не проходит, стрелки могут располагаться произвольно. Следовательно, расстановок, при которых на τ_n будет точно j ошибок, имеется всего $2^{2^k-1-k} C_k^j$.

Образуем теперь сумму:

$$P_j = \sum_{n=2^k+1}^{2^{k+1}} p\left\{\text{среди первых } k \text{ прогнозов } M \text{ на } \tau_n \text{ будет точно } j \text{ ошибок}\right\}.$$

Эта сумма состоит из $2^k \times 2^{2^k-1-k} C_k^j = 2^{2^k-1} C_k^j$ слагаемых. Здесь имеется, конечно, много повторений. Однако в силу полной симметрии все слагаемые $P(A_i)$ повторяются одинаковое число раз. Значений i всего 2^{2^k-1}, поэтому каждое $P(A_i)$ повторяется ровно C_k^j раз. Сумма всех $P(A_i)$, взятых по одному, равна 1, поэтому вся сумма $P_j = C_k^j$.

Если через $Q_n \; (2^k < n \leq 2^{k+1})$ обозначить вероятность того, что среди первых k прогнозов M на τ_n не менее j ошибок, то сумма всех Q_n равна $C_k^j + C_k^{j+1} + \dots + C_k^k$. Поэтому одна вероятность Q_n обладает свойством:

$$Q_n \geq 2^{-k} \sum_{s=j}^{k} C_k^s.$$

Итак, для данной В-стратегии M при любых k, j, таких, что $0 \leq j \leq k$, из функций $\tau_n \; (2^k < n \leq 2^{k+1})$ можно выбрать такую τ_n, что

$$p\left\{M, \tau_n, \geq j\right\} \geq 2^{-k} \sum_{s=j}^{k} C_k^s.$$

Отсюда при $j = \left]\frac{k+1}{2}\right[$ получаем:

$$p\left\{M, \tau_n, \geq \frac{k+1}{2}\right\} \geq \frac{1}{2}.$$

Так как $k+1 \geq \log_2 n$, то теорема I доказана.

Для получения **верхних** оценок мы используем только В-стратегии с независимыми прогнозами. Окончательный результат выражает .

ТЕОРЕМА 2. Для каждого нумерованного класса (U,τ) можно построить всюду финитную и рекурсивную В-стратегию R, прогнозы которой независимы и которая прогнозирует любую $\varphi \in U$; и при этом:

$$\lim_n P\left\{R, \tau_n, \leq \frac{1}{2}\log_2 n + \sqrt{\log n}\,\log\log n\right\} = 1.$$

ДОКАЗАТЕЛЬСТВУ теоремы 2 посвящена оставшаяся часть этой статьи.

Заметим сначала, что если M - стратегия с независимыми прогнозами, то для получения оценки вида:

$$\lim_n P\left\{M, \tau_n, \leq f(n) + \sqrt{f(n)}\,\log f(n)\right\} = 1$$

достаточно получить сначала оценку суммы вероятностей ошибок:

$$\sum_m P_m\left\{M, \tau_n\right\} \leq f(n).$$

Это следует из леммы 2.

ЛЕММА 2. Если прогнозы В-стратегии M на функции φ независимы и $\sum_m P_m\left\{M, \varphi\right\} \leq a$, то

$$P\left\{M, \varphi, \leq a + \sqrt{a}\,\log a\right\} = 1 - \varepsilon(a),$$

где $\varepsilon(a) = o(1)$ при $a \to \infty$.

ДОКАЗАТЕЛЬСТВО. Введем случайные величины:

$$x_m = \begin{cases} 1, & \text{если } M(\varphi, m) \neq \varphi(m+1), \\ 0, & \text{если } M(\varphi, m) = \varphi(m+1). \end{cases}$$

По условию леммы x_m независимы и $\sum_m P\{x_m=1\}\leq a$. Из неравенства Чебышева вытекает, что в этих условиях при $a\to\infty$

$$P\left\{\sum_{1}^{\infty} x_m > a+\sqrt{2a\ln a}\right\}\to 0$$

Так как $\sum\limits^{1} x_m$ - число ошибок, допускаемых стратегией M на функции φ , то лемма 2 доказана.

§ 3. Доказательство теоремы 2 (нерекурсивный вариант)

Мы должны для каждого нумерованного класса (U,τ) построить рекурсивную В-стратегию R , которая прогнозировала бы любую $\tau_n\in U$, причем допуская как правило не более $\frac{1}{2}\log_2 n$ ошибок. Леммы I,2 позволяют вначале сосредоточить все усилия на оценке суммы вероятностей ошибок $\sum_m P_m\{R,\tau_n\}$ (как функции от n). Кроме того, в этой первой части доказательства мы игнорируем требование финитности и рекурсивности искомой В-стратегии R . Этим требованиям посвящен § 4.

Пусть требуется прогнозировать некоторую функцию φ из класса U . Какие вероятностные предположения об этой функции можно сделать еще до получения первого значения $\varphi(0)$? Может быть, φ выбрана из U "случайно"? Попытаемся приписать каждому τ -номеру n некоторую "априорную" вероятность $\pi_n>0\left(\sum\pi_n=1\right)$. (Эта идея принадлежит Р. Фрейвалду [4,6] .) Имея распределение $\pi=\{\pi_n\}$, мы можем вычислить,"с какой вероятностью" функция φ , "случайно" (в соответствии с распределением π) выбранная из нумерации τ , будет принимать значение $\varphi(0)=t$. Для каждого $t\in N$ эта вероятность суть

$$\varkappa_t=\sum\left\{\pi_n \mid \tau_n(0)=t\right\},$$

где пустая сумма считается $=0$. Тогда в качестве прогноза мы могли бы выдать 0 с вероятностью $\varkappa_0$, 1 - с вероятностью $\varkappa_1$, и т.д. Дальнейшие прогнозы (когда уже получены некоторые значения $\varphi(0) \dots \varphi(m)$) могут определяться тем же способом, только вместо полных вероятностей приходится брать условные.

Таким образом, каждой нумерации τ и каждому распределению вероятностей π (где $\pi_n > 0$, $\sum \pi_n = 1$) естественным образом соответствует некоторая В-стратегия $Q_{\tau\pi}$.

Определение прогноза $Q_{\tau\pi}(\varphi, m)$, $m \geqslant -1$. Для каждого $t \in N$ берется вероятность

$$\varkappa_t = \sum \left\{ \pi_n \,/\, \tau_n(m+1) = t \wedge (\forall x \leqslant m)\, \tau_n(x) = \varphi(x) \right\}.$$

Если сумма $\varkappa = \sum \varkappa_t > 0$, то полагаем $Q_{\tau\pi}(\varphi, m) = t$ с вероятностью $\varkappa_t / \varkappa$. Если же $\varkappa = 0$, то пусть $Q_{\tau\pi}(\varphi, m) = \infty$ с вероятностью 1.

Если добавить, что прогнозы определяются независимо друг от друга, то В-стратегию $Q_{\tau\pi}$ можно определить на каком-либо одном вероятностном пространстве (Ω, B, P) (см. [2]).

Оказывается, что В-стратегия $Q_{\tau\pi}$ обладает следующим свойством: для всех n

$$\sum_m P_m \left\{ Q_{\tau\pi}, \tau_n \right\} \leqslant \ln \frac{1}{\pi_n}.$$

Чтобы доказать это, проще всего положить в лемме 3 (см. ниже): $\lambda(x) = x$, $c = \ln 2$. Таким образом, стратегия $Q_{\tau\pi}$ тем лучше, чем медленнее стремится к нулю π_n при $n \to \infty$. Но этот процесс не может быть произвольно медленным, он связан условием $\sum \pi_n = 1$. Поэтому мы не можем взять $\pi_n = const$ и даже не $\pi_n \sim \frac{1}{n}$, однако допустимо выбрать (считая, что $1/0 = 1$):

$$\pi_n^0 = \frac{b}{n(\ln n)^2},$$

где $\sum \pi_n^{\circ} = 1$. Полученная стратегия $Q_{\tau\pi^\circ}$ обладает свойством

$$\sum_m P_m\{Q_{\tau\pi}, \tau_n\} \leq \ln n + O(\log \log n).$$

Это примерно $0{,}694 \log_2 n$. Причем дело здесь не в методе оценки, а в самой стратегии $Q_{\tau\pi^\circ}$. Можно показать, что если взять нумерацию τ°, где $\tau_n^\circ = 0^n 1 0^\infty$ то для соответствующей В-стратегии $Q_{\tau^\circ\pi^\circ}$ при любом $\varepsilon > 0$ мы будем иметь:

$$\lim_{n \to \infty} P\{Q_{\tau^\circ\pi^\circ}, \tau_n^\circ, \leq (1-\varepsilon) \ln n\} = 0.$$

Таким образом, естественный метод построения прогнозирующей В-стратегии оказывается неоптимальным.

Выход из положения состоит во введении дополнительной (к распределению π) "степени свободы" - некоторой функции $\lambda(x)$ действительного переменного, определенной на отрезке $[0,1]$. Эта функция должна обладать свойствами:

$$(\forall x)(0 < x < 1 \to 0 < \lambda(x) < 1),$$
$$(\forall i)\, x_i \geq 0 \wedge \sum x_i \leq 1 \to \sum \lambda(x_i) \leq 1 \qquad (1)$$

для того, чтобы ее можно было использовать в определении следующей В-стратегии $Q_{\tau\pi\lambda}$.

Определение прогноза $Q_{\tau\pi\lambda}(\varphi, m)$, $m \geq -1$. Для каждого $t \in N$ берется вероятность

$$\varkappa_t = \sum\{\pi_n / \tau_n(m+1) = t \wedge (\forall x \leq m)\tau_n(x) = \varphi(x)\}.$$

Если $\varkappa = \sum \varkappa_t = 0$, то $Q_{\tau\pi\lambda}(\varphi, m) = \infty$ с вероятностью 1. Если же $\varkappa > 0$, то $Q_{\tau\pi\lambda}(\varphi, m) = t$ с вероятностью $\lambda(\varkappa_t/\varkappa)$ (ср. с вероятностью $\varkappa_t/\varkappa$ у стратегии $Q_{\tau\pi}$). Причем, если

$$\sum_t \lambda\left(\frac{\varkappa_t}{\varkappa}\right) = \varkappa' < 1,$$

то дополнительно выдается 0 с вероятностью $1-\varkappa'$.

В определении $Q_{\tau\pi\lambda}$ мы можем изменять функцию $\lambda(x)$, соблюдая только условие (I). К чему следует стремиться при этом, показывает лемма 3.

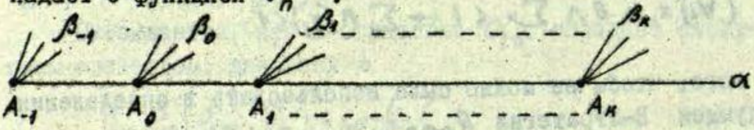
ЛЕММА 3. Пусть даны: (а) нумерация τ, (б) распределение π, где $\pi_n>0$ для всех n и $\sum \pi_n = 1$, (в) функция λ, обладающая свойством (I), а также свойством:

$$0<x\leq 1 \to 1-\lambda(x) < c\log_2\frac{1}{x}, \tag{2}$$

где $c>0$ – постоянная. Тогда В-стратегия $Q_{\tau\pi\lambda}$ обладает свойством: для всех n

$$\sum_m P_m\left\{Q_{\tau\pi\lambda}, \tau_n\right\} < c\log_2\frac{1}{\pi_n}.$$

ДОКАЗАТЕЛЬСТВО. Возьмем дерево тех функций нумерации τ, каждая из которых до некоторого места совпадает с функцией τ_n:



Каждой точке этого дерева можно приписать вероятность того, что функция τ_i пройдет через эту точку, если i выбрано из N по распределению $\pi = \left\{\pi_i\right\}$. Через β_k обозначим вероятность того, что τ_i пройдет через точку A_k в с т о р о н у от τ_n. Через B_k обозначим сумму $\beta_k+\beta_{k+1}+\dots$. Всей ветке τ_n приписывается вероятность $\alpha=\sum\left\{\pi_i \mid \tau_i=\tau_n\right\}$. Очевидно, $\alpha\geq\pi_n$, $\alpha+B_{-1}\leq 1$,.

Для стратегии $Q_{\tau\pi}$ (без функции λ) мы имели бы для всех k :

$$P_k\left\{Q_{\tau\pi},\tau_n\right\} = \frac{\beta_k}{\alpha+B_k}.$$

Для стратегии же $Q_{\tau\pi\lambda}$ мы имеем

$$1-P_k\left\{Q_{\tau\pi\lambda},\tau_n\right\} = \lambda\left(1-\frac{\beta_k}{\alpha+B_k}\right) = \lambda\left(\frac{\alpha+B_{k+1}}{\alpha+B_k}\right).$$

Из (2) вытекает, что

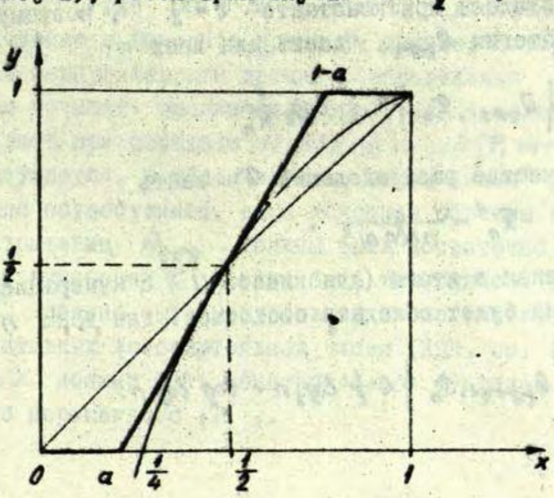
$$P_k\left\{Q_{\tau\pi\lambda},\tau_n\right\} < c\,\log_2\frac{\alpha+B_k}{\alpha+B_{k+1}}.$$

Суммируя:

$$\sum_k P_k\left\{Q_{\tau\pi\lambda},\tau_n\right\} < c\,\log_2\prod_k\frac{\alpha+B_k}{\alpha+B_{k+1}} = c\,\log_2\frac{\alpha+B_{-1}}{\alpha}.$$

Так как $\alpha+B_{-1}<1$ и $\alpha>\tau_n$, то лемма 3 доказана.

Итак, в интересах оптимальной оценки $\sum_m P_m\left\{Q_{\tau\pi\lambda},\tau_n\right\}$ мы должны искать функцию $\lambda(x)$ со свойством (I) такую, что (2) выполняется при возможно меньшей константе $c>0$. Так как $c<\frac{1}{2}$ заведомо невозможно (теорема I, см.§ 2), рассмотрим случай $c=\frac{1}{2}$.



Кривая на рисунке - это $y=1-\frac{1}{2}\log_2\frac{1}{x}$, при $x=\frac{1}{2}$ наклон ее касательной равен $\frac{1}{\ln 2}>1$. Если функция $\lambda(x)$ обладает свойством (2) с константной $c=\frac{1}{2}$, то ее график расположен н а д этой кривой. Простейший вариант - кусочно-линейная функция $\lambda^0(x)$, изображенная на рисунке $(a=\frac{1}{2}(1-\ln 2)\approx 0{,}153;\ 1-a\approx 0{,}847)$.

Покажем, что λ^0 обладает также свойством (I). Пусть $x_i>0$ для всех i и $\sum x_i<1$. Менее тривиален только один случай, когда для всех i : $a<x_i<1-a$. В этом случае имеем:

$$\sum_i \lambda^0(x_i)=\sum_i\left(\frac{1}{2}+(x_i-\frac{1}{2})\frac{1}{\ln 2}\right)<\frac{1}{\ln 2}\sum_i x_i-\frac{1}{2}\left(\frac{1}{\ln 2}-1\right)k,$$

где k - число слагаемых (очевидно, $k\leqslant 6$). Если $k=1$, то $\sum x_i<1-a$ и

$$\sum_i \lambda^0(x_i)<\frac{1}{\ln 2}\left(1-\frac{1-\ln 2}{2}\right)-\frac{1}{2}\left(\frac{1}{\ln 2}-1\right)=1.$$

Если же $k\geqslant 2$, то

$$\sum \lambda^0(x_i)<\frac{1}{\ln 2}-\frac{1}{2}\left(\frac{1}{\ln 2}-1\right)\cdot 2=1.$$

Итак, λ^0 обладает свойством (I). Свойством (2) эта функция обладает при константе $c=\frac{1}{2}$, поэтому лемма 3 для стратегии $Q_{\tau\pi\lambda^0}$ дает: для всех n

$$\sum_m P_m\left\{Q_{\tau\pi\lambda^0},\tau_n\right\}<\frac{1}{2}\log_2\frac{1}{\pi_n}.$$

Если в качестве распределения π взять

$$\pi_n^0=\frac{b}{n(\ln n)^2},$$

то полученная в итоге (для класса U с нумерацией τ) В-стратегия будет обладать свойством: для всех n

$$\sum_m P_m\left\{Q_{\tau\pi^0\lambda^0},\tau_n\right\}<\frac{1}{2}\log_2 n+\log\log n.$$

Из леммы I следует, что $Q_{\mathfrak{T}\pi^0\pi^0}$ прогнозирует любую функцию из U. Так как прогнозы этой стратегии независимы, то можно применить лемму 2 и получить, что

$$\lim_{n\to\infty} P\left\{ Q_{\mathfrak{T}\pi^0\pi^0}, \mathfrak{T}_n, \leq \frac{1}{2}\log_2 n + \sqrt{\log n}\,\log\log_n \right\} = 1,$$

т.е. $Q_{\mathfrak{T}\pi^0\pi^0}$ допускает на функции $\mathfrak{T}_n$, "как правило", не более $\frac{1}{2}\log_2 n$ ошибок.

Это почти то, что говорится в теореме 2, за исключением утверждения о существовании всюду финитной и рекурсивной В-стратегии с требуемым свойством.

§ 4. Доказательство теоремы 2 (финитный - рекурсивный вариант)

Каким образом из В-стратегии $Q_{\mathfrak{T}\pi\lambda}$ получить финитную и рекурсивную В-стратегию R, которая в смысле оценки $\sum_m P_m\left\{R, \mathfrak{T}_n\right\}$ (как функции от n) была бы ненамного хуже самой $Q_{\mathfrak{T}\pi\lambda}$? Основная идея (уже использованная в [5]) состоит в замене точного "вычисления" и "реализации" вероятностей вычислением и реализацией их двоично-рациональных приближений (т.е. приближений вида $s2^{-t}$, где $s,t \in N$; только такие вероятности и реализуемые в конечное время на машине, которая использует бернуллиевский датчик распределения $\frac{1}{2}, \frac{1}{2}$).
При этом точность реализации, естественно, следует быстро увеличивать при переходе от $R(\varphi, m)$ к $R(\varphi, m+1)$ и т.д.

Разумеется, в общем случае, чтобы такая "финитизация" была осуществимой, сами исходные объекты в определении стратегии $Q_{\mathfrak{T}\pi\lambda}$ должны быть достаточно конструктивными: нумерация $\mathfrak{T}$ должна быть вычислимой, распределение π должно быть рекурсивной последовательностью конструктивных действительных чисел (КДЧ, см. [7]), функция λ должна быть конструктивной функцией действительного переменного [7].

Оказывается, выполнение этих и еще одного условия достаточно, чтобы по данным τ, π, λ построить всюду финитивную и рекурсивную В-стратегию $R_{\tau\pi\lambda}$, которая по своим качествам произвольно мало уступает стратегии $Q_{\tau\pi}$ (см.роль функции $g(n)$ в лемме 4).

ЛЕММА 4. Пусть τ - вычислимая нумерация некоторого класса о.р.функций, π - рекурсивное распределение вероятностей на N ($\pi_n > 0$ для всех n, $\sum \pi_n = 1$), λ - неубывающая конструктивная функция на отрезке [0,I], обладающая свойством (I), свойством (2) при некоторой константе $c > 0$, а также следующим свойством: при некоторой константе $d > 0$

$$(\forall x\ \forall y) |\lambda(x) - \lambda(y)| < d|x-y|.$$

Пусть выбрана еще произвольная монотонная неограниченная о.р.функция $g(n)$. Тогда можно построить всюду финитную и рекурсивную В-стратегию R, прогнозы которой независимы и

$$(\exists a\ \forall n) \sum_m P_m\{R, \tau_n\} < c \log_2 \frac{1}{\pi_n} + g(n) + a.$$

ДОКАЗАТЕЛЬСТВО. Возьмем некоторую рекурсивную последовательность КДЧ $\bar{\varepsilon} = \{\varepsilon_m\}$, где

$$\forall_m (\varepsilon_m > \varepsilon_{m+1} > 0), \quad \sum_m \varepsilon_m < C < \infty.$$

Отправляясь от нумерации τ, распределения π, функции λ и от $\bar{\varepsilon}$, будем строить всюду финитную и рекурсивную В-стратегию $R_{\tau\pi\lambda\bar{\varepsilon}}$, которую для краткости обозначим через R. Затем, взяв функцию $g(n)$ и по ней, специально подобрав $\bar{\varepsilon}$, мы придем к искомой стратегии R в формулировке леммы 4.

Определение прогноза $R(\varphi, m)$, $m \geqslant -1$. Находим сначала s такое, что $\sum_{i>s} \pi_i < \varepsilon_m$. Если среди функций $\tau_1 \ldots \tau_s$ нет τ_i со свойством

$$(\forall x < m)\ \tau_i(x) = \varphi(x), \tag{3}$$

то полагаем $R(\varphi, m) = 0$ с вероятностью 1. Если же такие τ_i имеются, обозначим через P сумму всех π_i таких, что $1 \leqslant i \leqslant s$ и (3). Найдем σ такое, что $\sigma > s$ и $\sum_{i>\sigma} \pi_i < \varepsilon_m P$. Затем для каждого t вычисляем с недостатком сумму тех π_i, что $1 \leqslant i \leqslant \sigma$ и

$$\tau_i(m+1) = t \wedge (\forall x < m)\ \tau_i(x) = \varphi(x).$$

Каждый из недостатков следует сделать меньше $\varepsilon_m P$, а приближения непустых сумм следует выбрать отличными от нуля. Таким образом, получается конечная ($k \leqslant \sigma$) таблица значений t и соответствующих сумм с недостатком:

$$\begin{pmatrix} t_1 & \ldots & t_k \\ q_1 & \ldots & q_k \end{pmatrix},$$

где все q_j рациональны и > 0. Найдем теперь двоично-рациональные числа q_j' $(1 \leqslant j \leqslant k)$ со свойствами:

$$q_j' \geqslant \lambda\left(\frac{q_j}{q_1 + \cdots + q_k}\right) - \varepsilon_m,$$

$$\sum_1^k q_j' = 1.$$

Стратегия R полагает прогноз $R(\varphi, m)$ равным t_j с вероятностью q_j'. Определение закончено.

Элементарные выкладки приводят к заключению, что если $m \geqslant m_n$, где

$$m_n = \min\{m \mid \varepsilon_m < \pi_n\},$$

то

$$P_m\{R, \tau_n\} \le c \log_2 \frac{\alpha + B_m}{\alpha + B_{m+1}} + (2d+1)\varepsilon_m.$$

(Относительно α и B_m см. доказательство леммы 3.) Суммируя от -1 до ∞, получаем оценку

$$\sum_m P_m\{R, \tau_n\} \le (m_n + 1) + c \log_2 \frac{1}{\pi_n} + (2d+1)\sum_m \varepsilon_m.$$

Третье слагаемое постоянно. Если задаться функцией $g(n)$, последовательность $\bar{\varepsilon}$ легко подобрать настолько быстро убывающей, что

$$(\forall_n)(m_n \le g(n) + c').$$

Лемма 4 доказана.

Применим эту лемму к вычислимой нумерации τ и к распределению π°, где

$$\pi_n^{\circ} = \frac{b}{n(\ln n)^2},$$

а также к функции $\lambda^{\circ}(x)$ (определение этой кусочно-линейной функции см. § 3). Функцию $g(n)$ выберем равной $[\log \log n]$. Тогда все условия леммы 4 выполнены, $c = \frac{1}{2}$, $d = \frac{1}{\ln 2}$ (d - максимум производной λ°). Таким образом, мы получаем финитную и рекурсивную В-стратегию R, которая имеет на функции τ_n сумму вероятностей ошибок не более

$$\frac{1}{2}\log_2 n + C \log\log n,$$

где C - подходящая константа. Согласно лемме I R тогда прогнозирует любую τ_n, а в силу леммы 2 имеет место:

$$\lim_n P\{R, \tau_n, \le \frac{1}{2}\log_2 n + \sqrt{\log n}\, \log\log n\} = 1.$$

Теорема 2 доказана.

§ 5. Заключение

Согласно теореме 2 для любого нумерованного класса (U,τ) можно построить всюду финитную и рекурсивную В-стратегию R такую, что:

(а) при прогнозировании любой функции из класса U R допускает с вероятностью 1 не более, чем конечное число ошибок,

(б) если n -большое число, то R допускает на функции τ_n не более, чем $\frac{1}{2}\log_2 n+\sqrt{\log n}\,\log\log n$ ошибок с вероятностью, близкой к 1.

Теорема I показывает, что эту оценку нельзя (в общем случае) улучшить до $\frac{1}{2}\log_2 n-1$.

Сравним это с результатами, полученными Я.М.Барздинем и Р.В.Фрейвалдом [4,6] о детерминированных (Д) стратегиях.

I. Для любого нумерованного класса можно построить общерекурсивную Д-стратегию, которая допускает на n -ой функции не более $\log_2 n+\log\log n$ ошибок.

2. Существует нумерованный класс такой, что любая Д-стратегия вынуждена (для бесконечно многих n) допускать на n -ой функции не менее $\log_2 n$ ошибок.

Итак, получается как бы "уменьшение числа ошибок вдвое" при переходе от Д-стратегий к В-стратегиям. Приведем, однако, еще один результат. Будем оценивать (как функцию от n) среднее арифметическое число ошибок, допускаемых Д-стратегиями при прогнозировании первых n функций $\tau_1 \dots \tau_n$ класса U.

I. Для каждого нумерованного класса (U, τ) можно построить о.р.Д-стратегию, которая (при любом n) допускает на функциях $\tau_1 \dots \tau_n$ в среднем не более $0{,}585\log_2 n+O(1)$ ошибок.

2. Существует нумерованный класс (U , τ) такой, что любая Д-стратегия (при любом n) допускает на $\tau_1 \ldots \tau_n$ в среднем более $\frac{1}{2}\log_2 n - \frac{3}{2}$ ошибок.

Доказательство этих фактов мы опускаем. Имеются доводы в пользу того, что в верхней оценке $0{,}585$ можно будет заменить на $1/2$.

Таким образом, и Д-стратегии допускают "как правило" не более $\frac{1}{2}\log_2 n$ ошибок, наравне с В-стратегиями. Однако для всякой Д-стратегии может встретиться ситуация, когда для бесконечно многих n на функции τ_n число допускаемых ошибок определенно не меньше $\log_2 n$. Таких n "мало" (средняя ошибка $< \frac{1}{2}\log_2 n$), но на них Д-стратегия работает действительно плохо. В случае же В-стратегии с небольшой вероятностью число ошибок может превзойти $\frac{1}{2}\log_2 n$, но при $n \to \infty$ эта вероятность стремится к нулю.

ЛИТЕРАТУРА

1. Подниекс К.М. Сравнение различных типов предельного синтеза и прогнозирования функций. - "Учен. зап. Латв. ун-та", 1974, т.210.
2. Ламперти Дж. Вероятность. М., 1973.
3. Де Леу К., Мур Э.Ф., Шеннон К., Шапиро Н. Вычислимость на вероятностных машинах.-В кн.: Автоматы.М.,1956.
4. Барздинь Я.М., Фрейвалд Р.В. Прогнозирование общерекурсивных функций.-ДАН СССР,1972,т.206, № 3.
5. Барздинь Я.М. Предельный синтез τ-номеров.-"Учен. зап. Латв. ун-та", 1974, т.210.
6. Барздинь Я.М., Фрейвалд Р.В. Прогнозирование и предельный синтез эффективно перечислимых классов функций, там же.
7. Кушнер Б.А. Лекции по конструктивному математическому анализу. М., 1973.

РАСШИФРОВКА АВТОМАТОВ С ПОМОЩЬЮ ПРОСТЫХ ЭКСПЕРИМЕНТОВ ПРИ ОТСУТСТВИИ ВЕРХНЕЙ ОЦЕНКИ ЧИСЛА СОСТОЯНИЙ

Я.М.Барздинь

В [I] было показано, что существует эксперимент (как кратный, так и простой), расшифровывающий "большинство" конечных автоматов и в том случае, когда об этих автоматах верхняя оценка числа состояний не известна. Там же были получены и верхние оценки длины соответствующих экспериментов. В случае кратных экспериментов эти оценки носили достаточно окончательный вид. Однако в случае простых экспериментов разница между нижней и верхней оценкой была весьма значительной - соответственно κ и c^{κ}. Цель настоящей статьи - в случае простых экспериментов при равномерной (следовательно, и неравномерной) расшифровке получить верхнюю оценку длины эксперимента вида κ^{c} (κ -число состояний "черного ящика"). Этот результат был сформулирован без доказательства в [2].

Будем пользоваться понятиями и обозначениями из [I]. Напомним основные из них.

Под автоматами будем понимать обычные конечные инициальные автоматы, выход которых в любой момент может зависеть как от состояния, так и от входа в этот же момент. Предполагается, что все эти автоматы употребляют один и тот же входной алфавит $X=\{x_1, \dots, x_m\}$, где $m=const \geq 2$, и один и тот же выходной алфавит $Y=\{y_1, \dots, y_n\}$, где $n=const \geq 2$. Далее, будем считать (хотя это и не так существенно), что состояния автоматов занумерованы и равны соответственно $q_0, q_1, q_2, \dots$, где q_0, если не оговорено противное, является начальным состоянием. Оператор, который реализует автомат $\mathfrak{M}$ при начальном состоянии q_i, обозначим через $T_{\langle \mathfrak{M}, q_i \rangle}$.

Автоматы рассматриваются как "черные ящики", о внутренней структуре (в том числе и о верхней оценке числа состояний) которых ничего не известно (или известно, но при данной постановке не разрешается пользоваться). Предполагается, что с "черными ящиками" можно проводить простые эксперименты. Под а л г о р и т м о м Π п р о с т о г о э к с п е р и м е н т а н а д "ч е р н ы м и я щ и к а м и" ("алгоритмом расшифровки") понимается эффективное предписание, описывающее простой разветвленный эксперимент и указывающее, как по результату этого эксперимента строить соответствующий автомат (который предположительно работает также, как заданний "черный ящик"). Точнее, алгоритм Π, примененный к автомату $\mathfrak{M}$, работает по шагам. На каждом шаге алгоритм Π проделывает с автоматом $\mathfrak{M}$, находящимся в том состоянии, в котором он остался после предыдущего шага, некоторый простой однородный эксперимент, и в зависимости от результата этого эксперимента, а также результата экспериментов, проделанных на предыдущих шагах, делает одно из двух: а) или выдает результат $\Pi(\mathfrak{M})$ - некоторый автомат (например, в виде диаграммы); б) или строит новое входное слово, которое определяет простой эксперимент, проводимый на следующем шаге. Ясно, что алгоритм Π нигде не использует информацию о верхней оценке числа состояний автомата $\mathfrak{M}$. Состояние автомата $\mathfrak{M}$, в которое он переходит в результате применения алгоритма Π, обозначим через q_π. Будем говорить, что алгоритм Π расшифровывает автомат $\mathfrak{M}$, если $T_{\langle \Pi(\mathfrak{M}), q_0 \rangle} = T_{\langle \mathfrak{M}, q_\pi \rangle}$, т.е. если алгоритм Π однозначно определяет дальнейшее поведение автомата $\mathfrak{M}$.*)

---

*) В [I] данное понятие расшифровки названо остаточной расшифровкой.

Длину простого эксперимента, который проделывает алгоритм Π, примененный к $\mathfrak{M}$, обозначим через $\Pi^*(\mathfrak{M})$. Другими словами, $\Pi^*(\mathfrak{M})$ - общее число входных символов, вводимых в $\mathfrak{M}$, в процессе применения алгоритма Π. Положим

$$\Pi^*(k) = \max \Pi^*(\mathfrak{M})$$

где max берется по всем автоматам $\mathfrak{M}$, имеющим k состояний.

Пусть $\mathcal{L}$ - класс всех попарно неодинаковых автоматов (два автомата $\mathfrak{M}_1$ и $\mathfrak{M}_2$ мы считаем одинаковыми тогда и только тогда, когда любые два состояния с одинаковыми номерами как в диаграмме $\mathfrak{M}_1$, так и в диаграмме $\mathfrak{M}_2$ связаны между собой ребрами, одинаково ориентированными и с одинаковыми входными и выходными пометками). Пусть $\{\mathcal{L}_\lambda\}$ - некоторое разбиение $\mathcal{L}$ на конечные подклассы и $\mathcal{L}_\lambda^\Pi$ - множество тех автоматов из $\mathcal{L}_\lambda$, которые алгоритм Π расшифровывает. Рассмотрим отношение $P_\lambda = |\mathcal{L}_\lambda^\Pi| / |\mathcal{L}_\lambda|$ (через $|U|$ мы обозначаем мощность множества U). Будем говорить, что алгоритм Π расшифровывает автоматы с частотой $1-\varepsilon$ при данном разбиении $\{\mathcal{L}_\lambda\}$, если $P_\lambda \geqslant 1-\varepsilon$ для всех λ. В данной работе мы рассматриваем разбиение, при котором два автомата относятся к одному и тому же классу, если они отличаются только функциями выхода (такое разбиение будем называть разбиение по графу). Это разбиение является достаточно мелким. Поэтому из расшифровки с частотой $1-\varepsilon$ при данном разбиении следует расшифровка с частотой $1-\varepsilon$ при более крупных разбиениях, например, таких, как разбиение по числу состояний, когда любые два автомата относятся к одному подклассу, если они имеют одинаковое число состояний. Впредь говоря, что алгоритм Π *расшифровывает автоматы равномерно с частотой* $1-\varepsilon$, мы будем иметь в виду именно разбиение по графу. Под *автоматным графом* будем понимать граф, который получается из диаграммы автомата, если стереть выходные пометки (а входные оставить). Очевидно, из автоматного графа G с k вершинами, расставляя всевозможными способами выходные пометки, можно получить n^{mk} попарно неодинаковых автоматов. Класс таких автоматов обозначим через $\tilde{G}$. Таким образом, если алгоритм Π расшифровывает автоматы равномерно с частотой $1-\varepsilon$, то это означает, что для любого автоматного графа G имеет место

$$|\tilde{G}^{\Pi}| / |\tilde{G}| > 1-\varepsilon.$$

В дальнейшем алгоритмы на "черными ящиками", описывающие простые эксперименты, будем отождествлять с самими экспериментами и вместо "существует алгоритм Π, описывающий простой эксперимент" будем говорить "существует простой эксперимент Π".

ТЕОРЕМА. Для любого $\varepsilon > 0$ существует простой эксперимент Π, который расшифровывает автоматы равномерно с частотой $1-\varepsilon$ и имеет

$$\Pi^*(k) < k^c + c_\varepsilon,$$

где c - константа, не зависящая от k и ε, и c_ε -константа, не зависящая от k, но зависящая от ε.

Сначала напомним некоторые обозначения из [I], которые нам понадобятся при доказательстве теоремы:

$\langle \mathfrak{M}, q_i \rangle$ - автомат $\mathfrak{M}$ при фиксированном начальном состоянии q_i; если $q_i = q_0$, то вместо $\langle \mathfrak{M}, q_i \rangle$ обычно пишется просто $\mathfrak{M}$;

$T_{\langle \mathfrak{M}, q_i \rangle} x$ - выходное слово, в которое оператор $T_{\langle \mathfrak{M}, q_i \rangle}$ перерабатывает входное слово x;

$q_\alpha x$ - состояние автомата, в которое слово x переводит состояние q_α;

$|\mathfrak{M}|$ - число состояний автомата $\mathfrak{M}$;

$|G|$ - число вершин графа G ;

$D_{\langle G,q_i\rangle}(s)$ - спектр достижимости автомата (автоматного графа) $\langle G,q_i\rangle$ (см. с. 168 [I]);

$D_{\langle G,q_i\rangle}(x)$ - словарный спектр достижимости автомата (автоматного графа) $\langle G,q_i\rangle$ (см. с.308 [I]);

$F_{\langle \mathfrak{M},q_i\rangle}(x)$ - словарный спектр насыщения автомата $\langle \mathfrak{M},q_i\rangle$ (см. с. 308 [I]);

$\tilde{G}_{F_{q_i}(x)<s}$ - подмножество множества $\tilde{G}$, состоящее в точности из тех автоматов $\mathfrak{M}$, для которых $F_{\langle \mathfrak{M},q_i\rangle}(x)<s$ (см. с. 308 [I]).

Для доказательства теоремы нам понадобится ряд вспомогательных утверждений.

Будем считать, что произвольным образом фиксированы $\varepsilon>0$ и автоматный граф G .

ЛЕММА I. Пусть произвольным образом фиксированы натуральное число u , большее некоторого [*] u'_ε , и подмножество вершин U графа G такое, что $|U|\leqslant u^3$. Тогда для любого входного слова x по крайней мере $\left(1-\frac{\varepsilon}{u}\right)$-ая доля всех автоматов $\mathfrak{M}$ множества $\tilde{G}$ обладает следующим свойством A : какую бы вершину $q_i\in U$ мы ни брали, если $\bar{D}_{\langle G,q_i\rangle}(x)\geqslant u^2-8\log_n u-1$, то $\bar{F}_{\langle \mathfrak{M},q_i\rangle}(x)\geqslant u$.

Автомат $\mathfrak{M}\in\tilde{G}$ будем называть u -допустимым I при U , если для него имеет место свойство A из леммы 1 . Согласно лемме I, при $u>u'_\varepsilon$ и U , $|U|\leqslant u^3$, по крайней мере $\left(1-\frac{\varepsilon}{u}\right)$ -ую долю из всех автоматов множества $\tilde{G}$, составляют автоматы, являющиеся u -допустимыми I при U .

ДОКАЗАТЕЛЬСТВО ЛЕММЫ I. Пусть фиксированы натуральное число u , подмножество вершин U графа G , $|U|\leqslant u^3$, входное слово x и вершина q_i графа G ,

---

[*] Более точно это означает следующее: существует такое u'_ε, что как бы мы ни фиксировали натуральное u большее u'_ε , имеет место требуемое утверждение.

Согласно лемме I4 из главы IУ [I] ,

$$\frac{\left|\widetilde{G}_{F_{q_i}(x)<u}\right|}{|\widetilde{G}|} \leqslant \frac{(nu)^{mu}}{n^{D_{\langle G,q_i\rangle}(x)-1}}.$$

Обозначим через U' подмножество U , состоящее из всех тех вершин q_i , для которых $\bar{D}_{\langle G,q_i\rangle}(x) \geqslant u^2-8\log_n u^{-1}$, а через $\widetilde{G}_{U',F(x)<u}$ - множество всех тех автоматов $\mathfrak{M}$ из G , у которых существует хотя бы одна вершина $q_i \in U'$ такая, что $F_{\langle\mathfrak{M},q_i\rangle}(x)<u$. Очевидно,

$$\frac{\left|\widetilde{G}_{U',F(x)<u}\right|}{|\widetilde{G}|} \leqslant |U'| \max_{q_i\in U'} \frac{\left|\widetilde{G}_{F_{q_i}(x)\leqslant u}\right|}{|\widetilde{G}|} \leqslant u^3 \cdot \frac{(nu)^{mu}}{n^{u^2-8\log_n u-1}}.$$

Отсюда следует, что при u , больших некоторого u'_ε ,

$$\left|\widetilde{G}_{U',F(x)<u}\right| / |\widetilde{G}| \leqslant \frac{\varepsilon}{u}$$

или, что то же самое, по крайней мере $\left(1-\frac{\varepsilon}{u}\right)$ -ая доля из всех автоматов множества $\widetilde{G}$ обладает свойством A из леммы I. Лемма доказана.

ЛЕММА 2. Пусть s и k - произвольные натуральные числа. Тогда можно эффективно построить входное слово $B_s(k)$ длины $[4km^{s+2}\ln 2k]$, обладающее следующим свойством: какой бы автоматный граф G мы ни брали, если $D_{\langle G,q_i\rangle}(s)\geqslant k$ для любой вершины q_i графа G , то и $\bar{D}_{\langle G,q_i\rangle}(B_s(k))\geqslant k$ для любой вершины q_i графа G .

ДОКАЗАТЕЛЬСТВО. Для доказательства леммы, очевидно, достаточно показать, что можно эффективно найти входное слово $B_s(k)$ длины $[4km^{s+2}\ln 2k]$, обладающее следующим свойством: какой бы автоматный граф G с $D_{\langle G,q_i\rangle}(\ell)\geqslant k$ $(i=0,1,2,\ldots)$ мы ни брали и как бы мы в нем ни отмечали $k-1$ вершин, включая q_0, всегда из вершины q_0 словом $b_s(k)$ можно достичь одной неотмеченной вершины (под вершинами, достижимыми словом b, мы здесь понимаем все вершины, которые лежат на пути, определяемом словом b). Сопоставим графу G с $k-1$ отмеченными вершинами вспомогательный граф G', который получается из графа G, если отбросить неотмеченные вершины, а ребра, исходящие из отмеченных вершин и входящие в неотмеченные вершины (эти ребра будем называть запретными), подсоединить к произвольной отмеченной вершине. Очевидно, в графе G' слово x достигает из вершины q_0 неотмеченной вершины тогда и только тогда, когда в графе G это же слово достигает из q_0 какого-нибудь запретного ребра. Так как для любой вершины q_i графа G имеет место $D_{\langle a, q_i \rangle}(s) \geqslant k$, то для любой вершины q_i графа G существует входное слово длины, не превосходящей s, которое в графе G' достигает из вершины q_i хотя бы одного запретного ребра. Рассуждая в точности так же, как при доказательстве леммы I из [2], нетрудно убедиться, что число входных слов длины $2ps$, которые в графе G' не достигают из вершины q_0 ни одного запретного ребра, не превышает $(m^{2s}-sm^{s-1})^p$. С другой стороны, так как $|G'|<k$, то число различных графов типа G' (различных с учетом фиксации запретных ребер и без учета нумерации вершин, отличных от q_0) меньше, чем $k^{mk}2^{mk}$, где k^{mk} - число неодинаковых автоматных графов с k вершинами, и 2^{mk} - число способов, которыми в графе G с k вершинами можно зафиксировать запретные ребра. Отсюда получаем, что число различных входных слов длины $2ps$, каждое из которых хотя бы в одном графе типа G' не достигает из вершины q_0 ни одного запретного ребра (или, что то же самое, хотя бы в одном графе G упомянутого выше типа при каком-нибудь способе фиксации $k-1$ отмеченных вершин не достигает из верши-

ны q_0 ни одной неотмеченной вершины), не превышает $k^{mk}2^{mk}(m^{2s}-sm^{s-1})^p$. Далее, рассуждая опять в точности так же, как при доказательстве леммы I из [2], получаем, что при $2ps=[4m^{s+1}\ln k^{mk}2^{mk}]-[4km^{s+2}\ln 2k]$ обязательно найдется хотя бы одно входное слово, не обладающее упомянутым выше свойством. Очевидно, это слово можно эффективно найти; оно будет искомым словом $b_s(k)$. Лемма доказана.

Через $D_{\langle G,q_i\rangle}$ обозначим число вершин графа G (автомата G), достижимых из вершины q_i входными словами. Будем говорить, что слово x о с т а т о ч н о р а з л и ч а е т состояния q_α, q_β автомата $\mathfrak{M}$, если в случае, когда $q_\alpha x \neq q_\beta x$, имеет место $T_{\langle \mathfrak{M},q_\alpha\rangle}x \neq T_{\langle \mathfrak{M},q_\beta\rangle}x$.

ЛЕММА 3. Для любого натурального u, большего некоторого u''_ε, можно эффективно построить входное слово $b(u)$ длины $l(b(u))<u^a$ (где a – некоторое положительное число, не зависящее от u и ε) такое, что для любого автоматного графа G и любого подмножества U его вершин, где $|U| \leqslant u^3$, по крайней мере $(1-\frac{\varepsilon}{u})$-ая доля из всех автоматов $\mathfrak{M}$ множества $\tilde{G}$ обладает следующим свойством B: какие бы два состояния q_α, q_β автомата $\mathfrak{M}$ мы ни брали, если эти состояния принадлежат U и по крайней мере одно из них (пусть это будет q_α) удовлетворяет условию $D_{\langle G,q_\alpha b(u)\rangle} \geqslant 8\log_n u$, то слово $b(u)$ остаточно различает состояния q_α, q_β.

Автомат $\mathfrak{M}\in\tilde{G}$ будем называть u-д о п у с т и м ы м II при U, если для него имеет место свойство B из леммы 3 (при слове $b(u)$ из леммы 3). Согласно лемме 3, при $u>u''_\varepsilon$ и $U, |U|\leqslant u^3$, по крайней мере $(1-\frac{\varepsilon}{u})$-ую долю из всех автоматов множества $\tilde{G}$ составляют автоматы, являющиеся u-допустимыми II

при u .

ДОКАЗАТЕЛЬСТВО ЛЕММЫ 3. Пусть q_α , q_β - произвольные две вершины графа G и b - входное слово такое, что $\bar{D}_{\langle G,q_\alpha\rangle}(b)\geq q$ (или $\bar{D}_{\langle G,q_\beta\rangle}(b)\geq q$), где q - некоторое число. Пусть в некотором автомате $\mathfrak{M}\in\tilde{G}$ слово b остаточно не различает состояния q_α , q_β , т.е. $T_{\langle \mathfrak{M},q_\alpha\rangle}b= T_{\langle \mathfrak{M},q_\beta\rangle}b$, а $q_\alpha b\neq q_\beta b$. Так как $\bar{D}_{\langle G,q_\alpha\rangle}(b)\geq q$ (или $\bar{D}_{\langle G,q_\beta\rangle}(b)\geq q$) и $q_\alpha b\neq q_\beta b$, то легко видеть, что в слове b не меньше чем q букв имеют (q_α, q_β) -первичное вхождение (определение (q_α,q_β)-первичного вхождения см. в [I] , с. 337). Отсюда и из лемм I и 2' главы У [I] следует, что доля тех автоматов из множества $\tilde{G}$, для которых слово b не различает (следовательно, и остаточно не различает) состояния q_α , q_β , не больше чем $\left(\frac{1}{n}\right)^q$. Пусть фиксировано подмножество вершин U графа G, $|U|\leq u^3$ (следовательно, число различных пар (q_α, q_β) вершин, принадлежащих U , не превосходит u^6), и пусть $b(u)$ - входное слово такое, что для любой вершины q_α графа G , для которой $D_{\langle G,q_\alpha\rangle}(b(u))\geq q$, имеет место $\bar{D}_{\langle G,q_\alpha\rangle}(b(u))\geq q$. Тогда из изложенного выше следует, что не более чем у $u^6\left(\frac{1}{n}\right)^q$ -ой доли из всех автоматов $\mathfrak{M}$ множества $\tilde{G}$ существуют такие два состояния q_α , q_β , принадлежащие U и удовлетворяющие условию $D_{\langle G,q_\alpha\rangle}(b(u))\geq q$ (или $D_{\langle G,q_\beta\rangle}(b(u))\geq q$), что слово $b(u)$ их остаточно не различает. Пусть теперь q такое, что $u^6\left(\frac{1}{n}\right)^q<\frac{\varepsilon}{u}$. При u , большем некоторого $\bar{u}_\varepsilon$, в качестве такого q можно брать $q=8\log_n u$. Поэтому лемма будет доказана, если мы докажем следующее утверждение:

При u , большем некоторого $\bar{u}_\varepsilon$, существует входное слово $b(u)$ длины $l(b(u))\leq u^a$ (где a не зависит от u и ε) такое, что для любого графа G и любой его вершины q_α , для которой $D_{\langle G,q_\alpha\rangle}(b(u))\geq 8\log_n u$, имеет место $\bar{D}_{\langle G,q_\alpha\rangle}(b(u))\geq 8\log_n u$.

Справедливость данного утверждения легко вытекает из леммы 2 при $s=\kappa=\eta_0=8\log_n u$. Для этого рассмотрим слово $b_{\eta_0}(\eta_0)$ из леммы 2. Пусть $D_{\langle G, q_\alpha b_{\eta_0}(\eta_0)\rangle} \geqslant \eta_0$. Тогда, не меняя путь, начинающийся с вершины q_α и соответствующий слову $b_{\eta_0}(\eta_0)$, граф G можно перестроить в другой граф G', у которого при $s=\kappa=\eta_0$ выполняются условия леммы 2, т.е. $D_{\langle G', q_i\rangle}(\eta_0) \geqslant \eta_0$ для любой вершины $q_i \in G'$. Поэтому, согласно лемме 2, $\bar{D}_{\langle G', q_\alpha\rangle}(b_{\eta_0}(\eta_0)) \geqslant \eta_0$. Так как по построению $\bar{D}_{\langle G', q_\alpha\rangle}(b_{\eta_0}(\eta_0)) = \bar{D}_{\langle G, q_\alpha\rangle}(b_{\eta_0}(\eta_0))$, то отсюда $\bar{D}_{\langle G, q_\alpha\rangle}(b_{\eta_0}(\eta_0)) \geqslant \eta_0$. Теперь легко видеть, что слово $b(u)=b_{\eta_0}(\eta_0)$ является искомым. Длина этого слова $l(b(u))=[4\eta_0 m^{\eta_0+2}\ln 2\eta_0]$ и, следовательно, при u большем некоторого $\bar{\bar{u}}_\varepsilon$ имеем $l(b(u))<u^a$, где a - число, не зависящее от u и ε.

Очевидно, слово $b(u)$ может быть также и эффективно построено. Лемма доказана.

Слово $b(u)$ из леммы 3 там, где это не вызывает недоразумений, обозначим просто через b. Далее, обозначим через b^s слово $\underbrace{bb\ldots b}_{s\ \text{раз}}$. Положим

$$b'(u)=b^{u^6}, \qquad b'^{-1}(u)=b^{u^6-1}.$$

Введем еще одно понятие. Пусть, начиная с некоторого состояния q_α автомата $\mathfrak{M}$ мы подаем слово $b'(u)$. В результате $\mathfrak{M}$ перейдет в состояние $q_\alpha b'(u)$. Обозначим через y выходное слово, которое выдает $\mathfrak{M}$ при подаче последнего b, т.е. $y=T_{\langle \mathfrak{M}, q_\alpha b'^{-1}(u)\rangle} b$. Слово y будем называть q_α -х а р а к т е р и с т и к о й состояния $q_\alpha b'(u)$. Пусть l - некоторый путь в графе G. Будем говорить, что l содержится в подмножестве вершин U, если все вершины, принадлежащие l, принадлежат также и U.

ЛЕММА 4. Пусть произвольным образом фиксированы натуральное число u, $u>u'''_\varepsilon$, подмножество вершин U графа G, $|U|<u^3$, и автомат $\mathfrak{M}\in\tilde{G}$, являющийся

u -допустимым U при U. Пусть далее q_α, q_β - произвольные два состояния автомата $\mathfrak{M}$ такие, что:

а) пути, начинающиеся с q_α и q_β изадаваемые словом $b'(u)$, содержатся в U;

б) по крайней мере для одного из этих состояний (пусть это будет q_α) $D_{\langle G, q_\alpha b'(u)\rangle} \geqslant 8 \log_n u$.

В таком случае состояния $q_\alpha b'(u)$ и $q_\beta b'(u)$ совпадают (т.е $q_\alpha b'(u) = q_\beta b'(u)$) тогда и только тогда, когда q_α - характеристика состояния $q_\alpha b'(u)$ совпадает с q_β - характеристикой состояния $q_\beta b'(u)$.

ДОКАЗАТЕЛЬСТВО. Пусть выполнены условия леммы. Для простоты $b'(u)$ обозначим через b'. Сначала рассмотрим случай, когда $q_\alpha b' = q_\beta b'$. Покажем, что тогда q_α -характеристика состояния $q_\alpha b'$ совпадает с q_β -характеристикой состояния $q_\beta b'$. Так как число различных пар состояний, принадлежащих U, меньше u^6 и слово b' содержит u^6 раз слово $b = b(u)$, то обязательно найдется $j, j < u^6$, такое, что $(q_\alpha b^j, q_\beta b^j) = (q_\alpha b', q_\beta b')$. Отсюда и видно, что q_α -характеристика состояния $q_\alpha b'$ совпадает с q_β -характеристикой состояния $q_\beta b'$.

Пусть теперь дано, что q_α - характеристика состояния $q_\alpha b'$ совпадает с q_β -характеристикой состояния $q_\beta b'$. Покажем, что $q_\alpha b' = q_\beta b'$. Так как q_α и q_β удовлетворяют условиям данной леммы и слово $b = b(u)$ из леммы 3, то по лемме 3 получаем, что слово b должно остаточно различать состояния $q_\alpha b'^{-1}$, $q_\beta b'^{-1}$. Но так как $q_\alpha b'$ и $q_\beta b'$ имеют одинаковые характеристики, то $T_{\langle \mathfrak{M}, q_\alpha b'^{-1}\rangle} b = T_{\langle \mathfrak{M}, q_\beta b'^{-1}\rangle} b$. Это означает, что обязательно $q_\alpha b' = q_\beta b'$ (так как в противном случае слово b не могло бы остаточно различать $q_\alpha b'^{-1}$, $q_\beta b'^{-1}$). Лемма доказана.

ЛЕММА 5. Пусть произвольным образом фиксированы натуральное число u и подмножество U графа G такое, что $|U| < u^3$. Тогда по крайней мере $(1-\frac{\varepsilon}{u})$-ая доля из всех автоматов $\mathfrak{M}$ множества $\tilde{G}$ обладает следующим свойством C: какие бы два состояния q_α, q_β автомата $\mathfrak{M}$, принадлежащие U, мы ни брали, если эти состояния различимы, то их различимость может быть установлена подходящим входным словом длины $r(u,\varepsilon) = 7\log_n u + \log_n \frac{1}{\varepsilon}$.

Автомат $\mathfrak{M} \in \tilde{G}$ будем называть u-допустимым $Ш$ при U, если для него имеет место свойство C из леммы 5. Согласно лемме 5, при U, $|U| < u^3$, по крайней мере $(1-\frac{\varepsilon}{u})$ -ую долю из всех автоматов множества $\tilde{G}$ составляют автоматы, являющиеся u-допустимыми $Ш$ при U.

ДОКАЗАТЕЛЬСТВО ЛЕММЫ 5. Обозначим через $\tilde{G}_{U,\rho>r}$ множество всех тех автоматов из $\tilde{G}$, у которых существуют хотя бы два состояния q_α, q_β, принадлежащие U, которые не различимы входными словами длины r, но различимы входными словами большей длины. Так как число различных пар состояний, принадлежащих U, не превосходи u^6, то, используя неравенство (5) из доказательства теоремы 5.I. [I], получаем

$$\frac{|\tilde{G}_{U,\rho>r}|}{|\tilde{G}|} < u^6\left(\frac{1}{n}\right)^r.$$

Пусть теперь $r(u,\varepsilon)$ такое, что $u^6\left(\frac{1}{n}\right)^{r(u,\varepsilon)} < \frac{\varepsilon}{u}$. Выражая отсюда $r(u,\varepsilon)$, получаем справедливость леммы 5.

Для формулировки следующей леммы введем еще некоторые понятия. Под r-скрестностью (или окрестностью радиуса r) вершины q_α графа G будем понимать совокупность всех тех вершин, которые достижимы из вершины q_α входными словами длины не более r. Будем говорить, что с л о в о x в ы х о д и т з а п р е д е л ы r -о к р е с т н о с т и в е р ш и н ы q_α , если вершина $q_\alpha x$ или какая-нибудь другая вершина, достижимая из q_α начальным куском слова x , не принадлежат r -окрестности q_α .

ЛЕММА 6. Пусть произвольным образом фиксированы натуральное число u , большее некоторого u''_ε , и подмножество U вершин графа G такое, что $|U|\leqslant u^3$. Тогда по крайней мере $(1-\frac{\varepsilon}{u})$ -ая доля из всех автоматов $\mathfrak{M}$ множества $\tilde{G}$ обладает следующим свойством D : какие бы два состояния q_α , q_β автомата $\mathfrak{M}$, принадлежащие U , мы ни брали, если эти состояния не различимы входными словами длины $r(u)-8\log_n u$, то для любого входного слова x , которое хотя бы для одного из этих состояний выходит за пределы окрестности радиуса $r(u)-8\log_n u$, состояния $q_\alpha x$ и $q_\beta x$ совпадают (т.е. $q_\alpha x = q_\beta x$).

Автомат $\mathfrak{M}\in\tilde{G}$ будем называть u -д о п у с т и м ы м IV п р и U , если для него имеет место свойство D из леммы 6. Согласно лемме 6, при $u>u''_\varepsilon$ и U , $|U|\leqslant u^3$,по крайней мере $(1-\frac{\varepsilon}{u})$ -ую долю из всех автоматов множества $\tilde{G}$ составляют автоматы, являющиеся u -допустимыми IV при U .

ДОКАЗАТЕЛЬСТВО ЛЕММЫ 6. Пусть фиксированы натуральное число u и подмножество U вершин графа G , $|U|\leqslant u^3$. Из леммы 5 вытекает, что при u , большем некоторого u'''_ε , по крайней мере $(1-\frac{\varepsilon}{u})$ -ая доля из всех автоматов $\mathfrak{M}$ множества $\tilde{G}$ обладает следующим свойством: какие бы два состояния автомата $\mathfrak{M}$, принадлежащие U , мы ни брали, если эти состояния не различимы входными словами длины $r(u)-8\log_n u$, то они не различимы и входными словами большей длины. Поэтому лемма 6 будет доказана, если мы докажем утверждение, отличающееся от утверждения леммы 6 тем, что в свойстве D вместо "не различимы входными словами длины $r(u)=8\log_n u$", стоит "не различимы произвольными входными словами". Заменяя такое утверждение его отрицанием, получаем, что лемма 6 будет доказана, если мы докажем следующее утверждение. При u, большем некоторого $\tilde{u}_\varepsilon$, не более чем $\frac{\varepsilon}{u}$ -ая доля всех автоматов $\mathfrak{M}$ множества $\tilde{G}$ обладает следующим свойством: существуют по крайней мере два состояния q_α, q_β автомата $\mathfrak{M}$, принадлежащие U и не различимые входными словами (все равно какой длины), и существует входное слово x, выходящее хотя бы для одного из этих состояний за пределы окрестности радиуса $r(u)=8\log_n u$ такое, что $q_\alpha x \neq q_\beta x$. Для проверки справедливости этого утверждения заметим следующее. Если $q_\alpha x \neq q_\beta x$ и слово x выходит за пределы r -окрестности вершины q_α, то по крайней мере r букв слова x имеют (q_α, q_β) -первичное вхождение. Отсюда, используя леммы I и 2' из главы У [I], получаем справедливость следующего утверждения: пусть фиксированы произвольные две вершины q_α, q_β графа G и пусть для них существует слово x такое, что $q_\alpha x \neq q_\beta x$ и хотя бы для одной из этих вершин слово x выходит за пределы ее r -окрестности; тогда не более чем $\text{У}\left(\frac{1}{n}\right)^r$-ой доли из всех автоматов $\mathfrak{M}$ множества $\tilde{G}$ состояния q_α, q_β будут неразличимыми. Так как число различных пар вершин, принадлежащих U, не больше чем u^6, то из предыдущего утверждения получаем справедливость следующего утверждения: не более чем $u^6\left(\frac{1}{n}\right)^r$ -ая доля из всех автоматов $\mathfrak{M}$ множества $\tilde{G}$ обладает тем свойством, что существуют по крайней мере два состояния q_α, q_β автомата $\mathfrak{M}$, принадлежащие U и не различимые входными словами, и существует входное слово x, выходящее хотя бы для одного из этих состояний за пределы окрестности радиуса r, такое, что $q_\alpha x \neq q_\beta x$. Пусть теперь $r(u)=8\log_n u$. Тогда, очевидно, при u, большем некоторого $\tilde{u}_\varepsilon$, будет иметь место неравенство $u^{6}\left(\frac{1}{n}\right)^{r(u)} < \frac{\varepsilon}{u}$. Отсюда следует справедливость требуемого утверждения. Лемма доказана.

Пусть $x_1, x_2, \ldots, x_m$, как и выше, буквы входного алфавита. Будем считать, что $x_1 < x_2 < \cdots < x_m$. Под л е к с и к о г р а ф и ч е с к и м у п о р я д о ч е н и е м входных слов будем понимать следующее упорядочение: сначала идут входные слова длины I, затем входные слова длины 2, затем длины 3 и т.д., а среди входных слов $\zeta = x(1)\ldots x(t)$, $\zeta' = x'(1)\ldots x'(t)$ одинаковой длины t раньше идет слово ζ , если существует такое $j \leq t$, что $x(1) = x'(1), \ldots, x(j-1) = x'(j-1)$, а $x(j) < x'(j)$. Если при лексикографическом упорядочении слово ζ стоит раньше слова ζ' , то будем говорить, что ζ меньше ζ' .

Пусть $\mathfrak{M}$ - произвольный автомат, принадлежащий $\hat{a}$, q_i - произвольная вершина (состояние) графа G (автомата $\mathfrak{M}$) и r - произвольное натуральное число. Мы теперь определим две последовательности входных слов: одно - исходя из графа G , второе - исходя из автомата $\mathfrak{M}$. Будем считать, что вершины графа G (автомата $\mathfrak{M}$), достижимые из q_i входными словами, разбиты по ярусам: 0-ой ярус состоит из вершины q_i , h-ый ярус $(h = 1, 2, \ldots)$ - из всех тех вершин, которые достижимы из q_i входными словами длины h , но не достижимы входными словами меньшей длины. Далее, будем считать, что все эти вершины упорядочены:

$$q^{(1)}, q^{(2)}, \ldots, q^{(\ell)}, \ldots ,$$

где сначала идет вершина 0-ого яруса, затем вершины I-го яруса, затем 2-го яруса и т.д., а вершины одного и того же яруса h упорядочены так, что сначала идут вершины, в которые ведут ребра из I-ой вершины $(h-1)$-го яруса, затем вершины, в которые ведут ребра из 2-ой вершины $(h-1)$-го яруса и т.д., причем среди вершин, соответствующих одной и той же вершине q $(h-1)$-го яруса, раньше идут те, в которые ведут ребра из q, помеченные меньшими входными буквами. Под адресом $\zeta_{\langle\mathfrak{M},q_i\rangle}(q)$ (или $\zeta_{\langle G,q_i\rangle}(q)$) вершины q относительно q_i будем понимать наименьшее входное слово ζ (согласно лексикографическому упорядочению), при котором $q_i\zeta=q$. Очевидно введенное выше упорядочение $q^{(1)}, q^{(2)}, \ldots, q^{(l)}, \ldots$ - это упорядочение вершин в лексикографическом порядке их адресов. Под $(r+1)$-последовательностью ω_{r+1} входных слов будем понимать лексикографическую последовательность всевозможных входных слов длины не более $r+1$:

$$\nu_1, \nu_2, \ldots, \nu_v \qquad (v=m+m^2+\cdots+m^{r+1}).$$

Обозначим через $\zeta_{\langle\mathfrak{M},q_i\rangle}(q)\,\omega_{r+1}$ последовательность входных слов, которая получается из ω_{r+1}, если в начале каждого слова $\nu\in\omega_{r+1}$ приписать слово $\zeta_{\langle\mathfrak{M},q_i\rangle}(q)$. Определим теперь последовательность входных слов

$$g(G,q_i,r)=\left\{\zeta_{\langle\mathfrak{M},q_i\rangle}(q^{(1)})\,\omega_{r+1}, \zeta_{\langle\mathfrak{M},q_i\rangle}(q^{(2)})\,\omega_{r+1}, \ldots, \zeta_{\langle\mathfrak{M},q_i\rangle}(q^{(l)})\,\omega_{r+1}, \ldots\right\}.$$

Последовательность $g(G,q_i,r)$, очевидно, может быть эффективно построена, если в нашем распоряжении имеется граф G или диаграмма автомата $\langle\mathfrak{M},q_i\rangle$. Однако если автомат $\langle\mathfrak{M},q_i\rangle$ представляет собой "черный ящик" (хотя и с "возвратной кнопкой"), то по нему (используя только опрос) последовательность $g(G,q_i,r)$ не всегда может быть построена. Мы сейчас построим другую последовательность входных слов $-m(\mathfrak{M},q_i,r)$, в некотором смысле близкую $g(G,q_i,r)$, но уже обладающую тем свойством, что каждый следующий ее член может быть эффективно построен, используя опрос автомата $\langle\mathfrak{M},q_i\rangle$ предыдущими членами этой последовательности. Построение этой последовательности будет связано с построением некоторого автомата $\langle\mathfrak{M}',q_i\rangle$. Для удобства дальнейших рассуждений автомат $\langle\mathfrak{M}',q_i\rangle$ мы сначала построим, используя диаграмму автомата $\langle \mathfrak{M}, q_i \rangle$, а затем покажем, что этот же автомат (с точностью до нумерации состояний) может быть построен, используя только опрос автомата $\langle \mathfrak{M}, q_i \rangle$.

Автомат $\langle \mathfrak{M}', q_i \rangle$ будем строить поярусно, используя вершины и ребра (вместе с входными и выходными пометками на них) диаграммы автомата $\langle \mathfrak{M}, q_i \rangle$. Вершина q_i , также как и в автомате $\langle \mathfrak{M}, q_i \rangle$, составляет 0-ой ярус и в автомате $\langle \mathfrak{M}', q_i \rangle$. Далее, пусть уже построены первые h ярусов автомата $\langle \mathfrak{M}', q_i \rangle$ и пусть

$$p_1, p_2, \dots, p_s$$

- вершины h -го яруса, выписанные в порядке следования (при лексикографическом упорядочении) их адресов относительно q_i как вершин автомата $\langle \mathfrak{M}', q_i \rangle$. Тогда построение $h+1$ -го яруса происходит следующим образом. Рассматриваем в автомате $\langle \mathfrak{M}, q_i \rangle$ вершины, в которые ведут ребра из вершин h -го яруса автомата $\langle \mathfrak{M}', q_i \rangle$ (это вершины вида $p_j x_\ell$). Упорядочиваем эти вершины следующим образом:

$$p_1x_1, p_1x_2, \dots, p_1x_m, p_2x_1, p_2x_2, \dots, p_2x_m, \dots, p_tx_1, p_tx_2, \dots, p_tx_m, \dots$$

и обозначим их соответственно через

$$p_1', p_2', \dots, p_{s'}', \dots$$

Начинаем с вершины p_1' . Если она, как вершина автомата $\langle \mathfrak{M}, q_i \rangle$, не отличима входными словами длины r от какой-нибудь из уже построенных вершин автомата $\langle \mathfrak{M}', q_i \rangle$ (пусть это будет вершина q ; при определении отличимости она тоже рассматривается как вершина автомата $\langle \mathfrak{M}, q_i \rangle$), то вершину p_1' вычеркиваем (за исключением случая, когда $p_1' = q$), а ребра, исходящие из вершин предыдущего яруса и входящие в эту вершину, подсоединяем к вершине q . Если p_1' отличима входными словами длины r от любой из уже построенных вершин автомата $\langle \mathfrak{M}', q_i \rangle$, то вершину p_1' вместе с ребрами, исходящими из вершин предыдущего яруса и входящими в p_1', относим к $(h+1)$ -ому ярусу автомата $\langle \mathfrak{M}', q_i \rangle$. Пусть таким образом мы уже просмотрели вершины $p_1', \ldots, p_j'$. Тогда с вершиной p_{j+1}' поступаем так же, как с вершиной p_1'. А именно, если p_{j+1}' неотличима входными словами длины r от какой-нибудь из уже построенных вершин автомата $\langle \mathfrak{M}', q_i \rangle$ (это может быть как вершина первых h, ярусов, так и вершина из уже построенной части $(h+1$ -го яруса), то p_{j+1}' вычеркиваем, а ребра, входящие в нее, подсоединяем к неотличимой от нее вершине. Если p_{j+1}' отличима входными словами длины r от любой из предыдущих вершин автомата $\langle \mathfrak{M}', q_i \rangle$, то p_{j+1}' вместе с ребрами, входящими в нее, относим к $(h+1)$ -ому ярусу автомата $\langle \mathfrak{M}', q_i \rangle$. Таким образом, каждая следующая вершина, которую мы присоединяем к автомату $\langle \mathfrak{M}', q_i \rangle$, имеет больший адрес (относительно q_i в $\mathfrak{M}'$), нежели предыдущие вершины автомата $\langle \mathfrak{M}', q_i \rangle$.

Из изложенного выше непосредственно вытекает

ЛЕММА 7. Если r - число, не меньшее степени различимости автомата $\langle \mathfrak{M}, q_i \rangle$, то $\langle \mathfrak{M}', q_i \rangle$ является приведенным автоматом для автомата $\langle \mathfrak{M}, q_i \rangle$ (следовательно, $T_{\langle \mathfrak{M}', q_i \rangle} = T_{\langle \mathfrak{M}, q_i \rangle}$).

Отметим еще некоторые свойства автомата $\langle \mathfrak{M}', q_i \rangle$. Во-первых ребра, которые существовали между вершинами, когда они еще были вершинами автомата $\langle \mathfrak{M}, q_i \rangle$, сохранены и в автомате $\langle \mathfrak{M}', q_i \rangle$. Во-вторых, в автомате $\langle \mathfrak{M}', q_i \rangle$, по сравнению с автоматом $\langle \mathfrak{M}, q_i \rangle$, между оставшимися вершинами добавлены некоторые новые ребра; эти ребра возникли в результате подсоединения ребер, входящих в вычеркнутые вершины, к более ранним вершинам автомата $\langle \mathfrak{M}', q_i \rangle$; при этом вершины, которые мы вычеркивали, всегда имели большие адреса, чем те вершины, к которым мы подсоединяли концы ребер, входящие в вычеркнутые вершины. Следовательно, в результате такой процедуры мы не могли уменьшить адреса оставшихся вершин (по сравнению с тем, каковы они были относительно q_i в первоначальном автомате $\langle \mathfrak{M}, q_i \rangle$. В-третьих, при построении $\langle \mathfrak{M}', q_i \rangle$ из $\langle \mathfrak{M}, q_i \rangle$ мы некоторые вершины автомата $\langle \mathfrak{M}, q_i \rangle$ вычеркивали. Такая операция, как легко видеть, тоже не может уменьшить адреса оставшихся вершин. Другие операции в процессе построения автомата $\langle \mathfrak{M}', q_i \rangle$ мы не использовали. Таким образом имеет место следующая

ЛЕММА 8. Любая вершина q, которая принадлежит как автомату $\langle \mathfrak{M}, q_i \rangle$, так и автомату $\langle \mathfrak{M}', q_i \rangle$, обладает тем свойством, что ее адрес относительно q_i в автомате $\langle \mathfrak{M}', q_i \rangle$ не меньше, чем ее адрес относительно q_i в автомате $\langle \mathfrak{M}, q_i \rangle$.

Для построения последовательности $m(\mathfrak{M}, q_i, r)$ выпишем теперь вершины автомата $\langle \mathfrak{M}', q_i \rangle$ в порядке их построения или, что то же самое, в порядке следования их адресов относительно q_i в $\langle \mathfrak{M}', q_i \rangle$:

$$s_1, s_2, \dots, s_t, \dots$$

Положим

$$m(\mathfrak{M}, q_i, r) = \left\{ \zeta_{\langle \mathfrak{M}', q_i \rangle}(s_1)\omega_{r+1}, \zeta_{\langle \mathfrak{M}', q_i \rangle}(s_2)\omega_{r+1}, \dots, \zeta_{\langle \mathfrak{M}', q_i \rangle}(s_t)\omega_{r+1}, \dots \right\}.$$

Легко видеть, что число членов (т.е. входных слов) последовательности $m(\mathfrak{M}, q_i, r)$ не превосходит κv, где κ -число вершин автомата $\mathfrak{M}$, достижимых из q_i, а v -число членов последовательности ω_{r+1} $(v = m + m^2 + \dots + m^{r+1})$. Таким образом

$$\kappa v < \kappa m^{r+2}. \qquad (I)$$

Длина одного члена последовательности $m(\mathfrak{M}, q_i, r)$ не превосходит

$$\max_{s_t} \ell(q_{\langle \mathfrak{M}', q_i \rangle}(s_t)) + r + 1 \leqslant \kappa + r \qquad (2)$$

Хотя выше мы и определили автомат $\langle \mathfrak{M}', q_i \rangle$ и последовательность $m(\mathfrak{M}, q_i, r)$, используя диаграмму автомата $\langle \mathfrak{M}, q_i \rangle$, однако нетрудно убедиться, что автомат $\langle \mathfrak{M}', q_i \rangle$ (с точностью до нумерации состояний) и вместе с тем и последовательность $m(\mathfrak{M}, q_i, r)$ могут быть последовательно построены, используя только опрос автомата $\langle \mathfrak{M}, q_i \rangle$ предыдущими членами последовательности $m(\mathfrak{M}, q_i, r)$. В самом деле, рассмотрим построение I-го яруса автомата $\langle \mathfrak{M}', q_i \rangle$. 0-ой ярус состоит из одной вершины q_i. Опрашивая автомат $\langle \mathfrak{M}, q_i \rangle$ всевозможными входными словами длины не более $r+1$ (т.е. последовательностью входных слов $\zeta_{\langle \mathfrak{M}, q_i \rangle}(q_i)\omega_{r+1}$), мы находим для каждой вершины вида $q_i x_\gamma$ (т.е. для каждой вершины I-го яруса автомата $\langle \mathfrak{M}, q_i \rangle$) полное дерево высоты r, согласованное с автоматом $\langle \mathfrak{M}, q_i x_\gamma \rangle$. Используя данное дерево, мы устанавливаем, какие из этих вершин отличимы входными словами длины r, и какие неотличимы. Отождествляя неотличимые вершины, мы находим I-ый ярус автомата $\langle \mathfrak{M}', q_i \rangle$ (с точностью до нумерации состояний). Пусть $p_1, p_2, \dots, p_s$ - вершины I-го яруса автомата $\langle \mathfrak{M}', q_i \rangle$, выписанные в порядке следования (при лексикографическом упорядочении) их адресов относительно q_i. Для построения 2-го яруса автомата $\langle \mathfrak{M}', q_i \rangle$ опрашиваем автомат $\langle \mathfrak{M}, q_i \rangle$ последовательностью входных слов

$$\zeta_{\langle \mathfrak{M}', q_i \rangle}(p_1)\omega_{r+1}, \zeta_{\langle \mathfrak{M}', q_i \rangle}(p_2)\omega_{r+1}, \dots, \zeta_{\langle \mathfrak{M}', q_i \rangle}(p_s)\omega_{r+1}$$

(эта последовательность в точности совпадает с соответствующей частью последовательности $m(\mathfrak{M}, q_i, r)$) и дальше поступаем аналогично как при построении I-го яруса. Продолжая такую процедуру до момента появления пустого яруса, мы построим (с точностью до нумерации состояний) автомат $\langle \mathfrak{M}', q_i \rangle$; $m(\mathfrak{M}, q_i, r)$ - это как раз та последовательность входных слов, которыми мы опрашивали автомат $\langle \mathfrak{M}, q_i \rangle$ в течение данной процедуры. Таким образом имеет место .

ЛЕММА 9. Для любого автомата $\langle \mathfrak{M}, q_i \rangle$ и любого натурального r автомат $\langle \mathfrak{M}', q_i \rangle$ (с точностью до нумерации состояний) и вместе с ним и последовательность $m(\mathfrak{M}, q_i, r)$ могут быть последовательно и эффективно построены, используя только опрос автомата $\langle \mathfrak{M}, q_i \rangle$ предыдущими членами последовательности $m(\mathfrak{M}, q_i, r)$.

Пусть $\tilde{g}(G, q_i, r)$ -некоторый начальный кусок последовательности слов $g(G, q_i, r)$. Через $\tilde{g}^*(G, q_i, r)$ обозначим множество вершин графа G, достижимых из q_i словами из $\tilde{g}(G, q_i, r)$. Пусть $\{\eta_1, \eta_2, \dots, \eta_j, \dots\}$ - некоторая последовательность входных слов. Член $\eta_j = x(1) \dots x(t)$ назовем в т о р и ч н ы м в этой последовательности, если для любого $\tau < t$ существует член η_s, $s<j$, что в графе G $q_i \eta_s = q_i x(1) \dots x(\tau)$.

ЛЕММА 10. Пусть u - произвольное натуральное число, U -подмножество вершин графа G такое, что $|U| < u^3$; q_i - вершина, принадлежащая U, и $r(u) = 8 \log_n u$. Пусть, далее, $\mathfrak{M}$ - произвольный автомат, принадлежащий $\tilde{G}$ и являющийся u-допустимым IУ при U. Тогда для любого начального куска $\tilde{g}(G, q_i, r(u))$ последовательности $g(G, q_i, r(u))$ такого, что $\tilde{g}^*(G, q_i, r(u)) \subseteq U$, имеет место следующее: существует некоторый начальный кусок последовательности $m(\mathfrak{M}, q_i, r(u))$ (минимальный такой кусок обозначим через $\tilde{m}(\mathfrak{M}, q_i, r(u))$), который может быть получен из $\tilde{g}(G, q_i, r(u))$ вычеркиванием некоторых вторичных членов и добавлением некоторых новых вторичных членов.

ДОКАЗАТЕЛЬСТВО. Под адресом вершины мы будем понимать ее адрес относительно q_i в G. Учтем, что в последовательностях $g(G, q_i, r)$ и $m(\mathfrak{M}, q_i, r)$ новые слова появляются в лексикографическом порядке и что в графе G вершины упорядочены в порядке следования при лексикографическом упорядочении их адресов: $q^{(1)}, q^{(2)}, \dots, q^{(\ell)}, \dots$. Кроме того, последовательность $g(G, q_i, r)$ содержит адреса всех вершин $q^{(1)}, \dots, q^{(\ell)}, \dots$ В частности, это означает, что $\tilde{g}^*(G, q_i, r(u))$ является начальным куском последовательности $q^{(1)}, q^{(2)}, \dots, q^{(\ell)}, \dots$. Поэтому лемма будет доказана , если при ее условиях мы докажем следующее утверждение:

А. Для любого ℓ такого, что множество первых ℓ вершин $\{q^{(1)}, \dots, q^{(\ell)}\}$ содержится в U , последовательность $m(\mathfrak{M}, q_i, r(u))$ содержит адреса вершин $\{q^{(1)}, \dots, q^{(\ell)}\}$.

Пусть ℓ_1 и ℓ_2 - два пути в графе G , начинающиеся с вершины q_i . Будем говорить, что ℓ_1 меньше ℓ_2 , если входное слово, которое "несет" ℓ_1 , меньше входного слова, которое "несет" ℓ_2 . Путь, ведущий из q_i в q , назовем минимальным, если он "несет" адрес вершины q . Пусть $q \in \{q^{(1)}, \dots, q^{(\ell)}\}$, где $\{q^{(1)}, \dots q^{(\ell)}\} \subset U$, и пусть

$$\mathfrak{P} = (q_i, v_1, v_2, \dots, v_p, v_{p+1}, \dots v_{p+r(u)}, q)$$

- минимальный путь в диаграмме автомата $\langle \mathfrak{M}, q_i \rangle$, ведущий из q_i в q (v_j - вершины, лежащие на этом пути; для простоты мы рассматриваем случай, когда длина пути больше $r(u)$). Очевидно, каждая вершина минимального пути принадлежит своему ярусу. Докажем следующее утверждение:

В. Вершины $q_i, v_1, v_2, \dots, v_p$ (т.е. все вершины пути $\mathfrak{P}$, кроме, быть может, последних $r(u)+1$ вершин) входят также и в автомат $\langle \mathfrak{M}', q_i \rangle$.

Предположим от противного, что это не так, т.е. что до некоторого $j < p$ вершины $q_i, v_1, v_2, \dots, v_{j-1}$ еще принадлежат $\langle \mathfrak{M}', q_i \rangle$, а вершина v_j уже не принадлежит $\langle \mathfrak{M}', q_i \rangle$. В таком случае должна существовать более ранняя вершина p автомата $\langle \mathfrak{M}', q_i \rangle$ (т.е. вершина, имеющая в $\langle \mathfrak{M}', q_i \rangle$ меньший адрес, чем v_j), неотличимая от v_j входными словами длины $r(u)$. Отсюда и из леммы 8 следует, что в автомате $\langle \mathfrak{M}, q_i \rangle$ (или, что то же самое, в графе G) вершина p должна иметь меньший адрес, чем вершина v_j. Но v_j имеет меньший адрес, чем q. Так как q принадлежит $\{q^{(1)}, \dots, q^{(l)}\}$, то отсюда получаем, что v_j и p тоже принадлежат $\{q^{(1)}, \dots, q^{(l)}\}$ и, следовательно, v_j и p принадлежат также и U. Далее, так как согласно условиям леммы, автомат $\mathfrak{M}$ является u-допустимым IУ при U, т.е. для него выполняется свойство D из леммы 6, то согласно лемме 6 получаем следующее: Пусть x - входное слово длины $r(u)+1$, которое "несет" кусок пути $\mathfrak{N}$, начинающийся с v_j (следовательно, x выходит за пределы $r(u)$-окрестности v_j); тогда $px = v_j x = v_{j+r(u)+1}$. Отсюда, так как p имеет меньший адрес, чем v_j, получаем, что путь $(q_i, \dots, p, \dots, \dots, v_{j+r(u)+1}, \dots, q)$ меньше, чем путь $\mathfrak{N} = (q_i, \dots, v_j, \dots, v_{j+r(u)+1}, \dots, q)$. Но это противоречит выбору пути $\mathfrak{N}$. Таким образом, утверждение В доказано.

Так как вершины $q_i, v_i, v_2, \dots, v_p$ принадлежат автомату $\langle \mathfrak{M}', q_i \rangle$, то автомату $\langle \mathfrak{M}', q_i \rangle$ принадлежат также и ребра, которые в автомате $\langle \mathfrak{M}, q_i \rangle$ соединяли эти вершины. Поэтому для любого $j \leq p$ адрес $\zeta_{\langle \mathfrak{M}', q_i \rangle}(v_j)$ не больше, чем адрес $\zeta_{\langle \mathfrak{M}, q_i \rangle}(v_j)$. Отсюда, используя лемму 8, получаем, что $\zeta_{\langle \mathfrak{M}', q_i \rangle}(v_j) = \zeta_{\langle \mathfrak{M}, q_i \rangle}(v_j)$. Но в таком случае как в $g(G, q_i, r(u))$, так и в $m(\mathfrak{M}, q_i, r(u))$ существует кусок $\zeta_{\langle \mathfrak{M}', q_i \rangle}(v_p)\, \omega_{r(u)+1} = \zeta_{\langle \mathfrak{M}, q_i \rangle}(v_p)\, \omega_{r(u)+1}$. Очевидно, один из элементов этого куска равен $\zeta_{\langle \mathfrak{M}, q_i \rangle}(q)$. Утверждение А и тем самым лемма IO доказаны.

Обозначим через $g(G, q_i, r)/_s$ (через $m(\mathfrak{M}, q_i, r/_s)$) s-ый член последовательности $g(G, q_i, r)$ (последовательности $m(\mathfrak{M}, q_i, r)$).

Для построения искомого эксперимента нам понадобятся некоторые специальные входные слова. Пусть a_0 - произвольная вершина графа G, r и u - произвольные натуральные числа. Сначала определим специальное входное слово $\mathcal{G}(G, a_0, r, u)$ (которое там, где это не вызывает недоразумений, будем обозначать просто через $\mathcal{G}$). При построении слова $\mathcal{G}(G, a_0, r, u)$ нам понадобится слово $b'(u)$ из леммы 4 (которое для простоты будем обозначать через b'). Слово $\mathcal{G}$ мы будем строить по шагам. Предварительно только отметим, что слово $\mathcal{G}$ будет иметь следующий вид:

$$\underbrace{b' \ldots b'}_{\text{шаг } 1} \underbrace{\eta_2 b' \ldots b' z_2}_{\text{шаг } 2} \underbrace{\eta_3 b' \ldots b' z_3}_{\text{шаг } 3} \ldots \ldots \underbrace{\eta_t b' \ldots b' z_t}_{\text{шаг } t} \ldots \ldots,$$

где η_t и z_t - специальные входные слова, которые будут определены ниже. Еще отметим, что одновременно со словом $\mathcal{G}$ мы будем строить некоторый граф P ; будем считать, что в начальный момент этот граф состоит только из одной вершины $a_{(0)}$.

Шаг I.*) В графе G , начиная с вершины a_0 , подаем слово b' . Вершину $a_0 b'$ обозначаем через p_1 . К графу P добавляем новую вершину $p_{(1)}$ (соответствующую вершине p_1 графа G), проводим ребро из $a_{(0)}$ в $p_{(1)}$ и помечаем это ребро словом b' . Затем опять в графе G , начиная с вершины p_1 , подаем слово b' и в результате достигаем вершины $p_1 b'$. Возможны два случая: I) $p_1 b'$ совпадает с p_1 и 2) $p_1 b'$ не совпадает с p_1 . Пусть имеет место второй случай. Тогда вершину $p_1 b'$ обозначаем через p_2 , а к графу P добавляем новую вершину $p_{(2)}$, проводим ребро из $p_{(1)}$ в $p_{(2)}$ и помечаем это ребро словом b' . Далее, в графе G , начиная с вершины p_2 , подаем слово b' , получаем вершину $p_2 b'$ и опять различаем два случая: I) $p_2 b'$ совпадает с какой-нибудь из предыдущих вершин p_1, p_2 и 2) $p_2 b'$ не совпадает ни с одной из предыдущих вершин. Пусть опять имеет место второй случай. Тогда вершину $p_2 b'$ обозначаем через p_3 , а к графу P добавляем новую вершину $p_{(3)}$, проводим ребро из $p_{(2)}$ в $p_{(3)}$

---

*) Этот шаг, по сравнению с остальными шагами, несколько вырожденный.

и помечаем это ребро словом b' . Такую последовательную подачу слов b' с последовательным выделением вершин $p_1 = a_0 b'$, $p_2 = p_1 b'$, $p_3 = p_2 b'$, $p_4 = p_3 b'$, ... и последовательным добавлением к графу P новых вершин $p_{(1)}$, $p_{(2)}$, $p_{(3)}$, $p_{(4)}$, ... и новых ребер, помеченных словом b' (рис. I), повторяем до такого j_1 , пока вершины $p_1, p_2, \dots, p_{j_1-1}$ все различны, а вершина p_{j_1-1} совпадает с какой-нибудь из предыдущих вершин (пусть это будет вершина p_{s_1}). Тогда в графе P новую вершину не добавляем, а лишь из $p_{(j_1-1)}$ проводим ребро в $p_{(s_1)}$ и это ребро, как и выше, помечаем словом b' . Вершину $p_{(s_1)}$ называем финальной вершиной шага I. Этим шаг I заканчивается. В его результате мы получаем слово $\underbrace{b' \dots b'}_{j_1 \text{ раз}}$. Затем переходим к шагу 2.

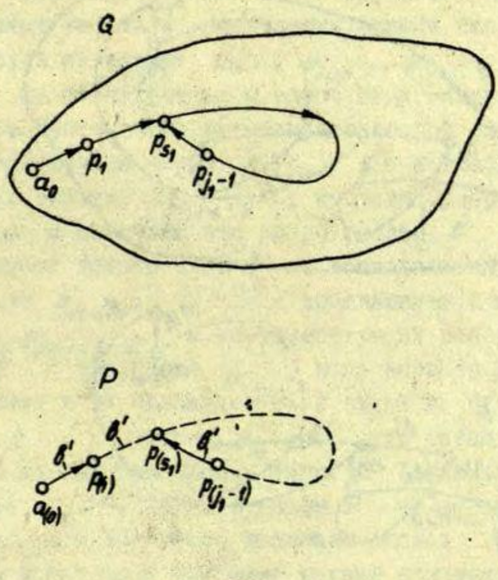


Рис. I.

Шаг t ($t=2,3,\ldots$). Пусть $p(s_{t-1})$ – финальная вершина предыдущего шага (то есть $p(s_{t-1})$ – вершина графа G ,на которой мы остановились в результате выполнения предыдущего шага) и пусть ℓ – число шагов среди первых $t-1$, для которых вершина $p(s_{t-1})$ была финальной. Тогда в графе G начиная с вершины $p_{s_{t-1}}$, подаем слово

$$\eta_t = g(G, p_{s_{t-1}}, r)/\ell \tag{3}$$

и достигаем вершины $a_t = p_{s_{t-1}}\eta_t$. Затем к графу P добавляем вершину $a_{(t)}$, проводим ребро из $p(s_{t-1})$ в $a_{(t)}$ и помечаем это ребро словом η_t (рис.2). Пусть

$$\underbrace{p_1,\ldots,p_{j_1-1},}_{\text{шаг } 1}\ \underbrace{a_2,p_{j_1},\ldots,p_{j_2-1},}_{\text{шаг } 2}\ \ldots\ \ldots,\ \underbrace{a_{t-1},p_{j_{t-2}},\ldots,p_{j_{t-1}-1}}_{\text{шаг } t-1}$$

– вершины графа G , выделенные на предыдущих шагах,

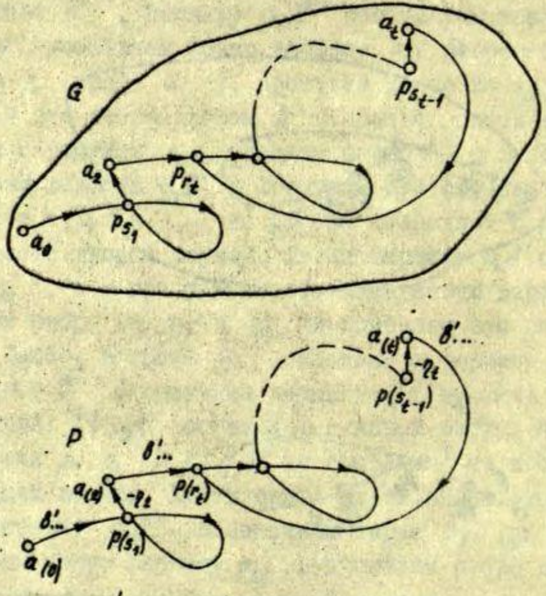


Рис. 2.

и пусть

$$p_{(1)}, \dots, p_{(j_1-1)}, a_{(2)}, p_{(j_1)}, \dots, p_{(j_2-1)}, \dots \dots, a_{(t-1)}, p_{(j_{t-2})}, \dots, p_{(j_{t-1}-1)}$$

- соответствующие вершины графа P (вершины $p_1, \dots, p_{j_1-1}, p_{j_1}, \dots$ и $p_{(1)}, \dots, p_{(j_1-1)}, p_{(j_1)} \dots$ будем называть вершинами типа p, а вершины $a_2, a_3, \dots$ и $a_{(2)}, a_{(3)}, \dots$ - вершинами типа a). Тогда в графе G, начиная с вершины a_t (в точности так же, как на шаге I, начиная с вершины a_0), подаем слово b'. Возможны два случая: I) $a_t b'$ совпадает с какой-нибудь из предыдущих вершин типа p (т.е. с какой-нибудь из $p_1, \dots, p_{j_{t-1}-1}$) и 2) $a_t b'$ не совпадает ни с одной из вершин типа p. Пусть имеет место второй случай. Тогда вершину $a_t b'$ обозначаем через $p_{j_{t-1}}$, а к графу P добавляем новую вершину $p_{(j_{t-1})}$, проводим ребро из $a_{(t)}$ в $p_{(j_{t-1})}$ и помечаем это ребро словом b'. Затем, начиная с вершины $p_{j_{t-1}}$ графа G, опять подаем слово b', и опять возможны два случая: I) $p_{j_{t-1}} b'$ совпадает с какой-нибудь из предыдущих вершин типа p (т.е. с какой-нибудь из вершин $p_1, \dots, p_{j_{t-1}-1}, p_{j_{t-1}}$) и 2) $p_{j_{t-1}} b'$ не совпадает ни с одной из предыдущих вершин типа p. Пусть опять имеет место второй случай. Тогда $p_{j_{t-1}} b'$ обозначаем через $p_{j_{t-1}+1}$, а к графу P добавляем новую вершину $p_{(j_{t-1}+1)}$, проводим ребро из $p_{(j_{t-1})}$ в $p_{(j_{t-1}+1)}$ и помечаем это ребро словом b'. Продолжаем такой процесс подачи слов b' с последовательным выделением вершин $p_{j_{t-1}}, p_{j_{t-1}+1}, \dots$ и добавлением к графу P вершин $p_{(j_{t-1})}, p_{(j_{t-1}+1)}, \dots$ и соответствующих ребер, помеченных словом b', до такого j_t, пока вершины $p_{j_{t-1}}, p_{j_{t-1}+1} \dots p_{j_t-1}$ все различны и не совпадают ни с одной из предыдущих вершин типа p, а вершина $p_{j_t-1} b'$ уже совпадает с какой-нибудь из предыдущих вершин типа p (обозначим эту вершину через p_{r_t}). Тогда в графе P из $p_{(j_t-1)}$ проводим ребро в $p_{(r_t)}$ и это ребро помечаем словом b'. Далее, обозначим через $p_{(s_t)}$ наиболее раннюю финальную вершину графа P такую, что в графе P из $p_{(r_t)}$ еще можно попасть в $p(s_t)$. Рассмотрим в графе P наиболее короткий ориентированный путь, который ведет из $p(r_t)$ в $p(s_t)$. Ребра этого пути, как и все ребра графа P , помечены либо словом b' , либо словом типа η . Выпишем эти слова-пометки одно за другим в порядке следования ребер в данном пути. Полученное слово обозначим через z_t (в частности, $p_{r_t} z_t = p_{s_t}$). Этим шаг t заканчивается. В его результате мы получаем слово $\eta \underbrace{b' \dots \dots b'}_{(l_t - l_{t-1}) \text{ раз}} z_t$ и достигаем вершины p_{s_t} . Соответствующий путь в графе G (он начинается с $p_{s_{t-1}}$, кончается на p_{s_t} и "несет" слово $\eta_t b' \dots \dots b' z_t$) называем путем, построенным на шаге t , а вершину $p(s_t)$ графа P - финальной вершиной шага t . Затем переходим к шагу $t+1$.

Описанную процедуру построения слова $\mathcal{G}$ мы продолжаем до такого шага t , что $\eta_t = g(G, p_{s_{t-1}}, r)\|_l$ (см. (3)) уже является пустым, т.е. все слова последовательности $g(G, p_{s_{t-1}}, r)$ уже перечислены на предыдущих шагах (в этом случае обязательно достигнуты все вершины графа G , которые вообще достижимы с помощью входных слов из финальной вершины $p_{s_{t-1}}$ шага $t-1$). Этим определение слова $\mathcal{G} = \mathcal{G}(G, a_0, r, u)$ заканчивается.

Слово $\mathcal{G}(G, a_0, r, u)$ было определено, используя последовательность слов $g(G, q, r)$. Пусть $\mathfrak{M}$ - произвольный автомат, принадлежащий $\tilde{G}$. Определим теперь входное слово $\mathcal{H}(\mathfrak{M}, a_0, r, u)$ в точности так же, как слово $\mathcal{G}(G, a_0, r, u)$, с той лишь разницей, что вместо графа G возьмем автомат $\mathfrak{M}$ и вместо последовательности $g(G, q, r)$ - последовательность $m(\mathfrak{M}, q, r)$. Вершины автомата $\mathfrak{M}$ и графа P , выделенные в процессе построения $\mathcal{H}(\mathfrak{M}, a_0, r, u)$, обозначим в точности так же, как соответствующие вершины, выделенные в процессе построения $\mathcal{G}(G, a_0, r, u)$.

Это значит, что шаг t процесса построения $\mathcal{H}(\mathfrak{M}, a_0, r, u)$ начинается с вершины $p_{s_{t-1}}$. Пусть l - число, указывающее, сколько раз вершина $p(s_{t-1})$ уже была финальной. Тогда $q_t = m(\mathfrak{M}, p_{s_{t-1}}, r)\|\ell$. Далее строятся вершины $a_t, p_{j_{t-1}}, \dots, p_{j_t-1}$ и слово z_t . Финальная вершина шага t также обозначается через $p_{(s_t)}$. Процесс построения слова $\mathcal{H}(\mathfrak{M}, a_0, r, u)$, как и процесс построения слова $\mathcal{G}(G, a_0, r, u)$, продолжается до такого шага t , что последовательность $m(\mathfrak{M}, p_{s_{t-1}}, r)$ уже полностью исчерпана и, следовательно, автомат $\langle \mathfrak{M}', p_{s_{t-1}} \rangle$, который строится вместе с последовательностью $m(\mathfrak{M}, p_{s_{t-1}}, r)$, уже полностью построен.

Вершину $p_{s_{t-1}}$, на которой заканчивается построение слова $\mathcal{H}(\mathfrak{M}, a_0, r, u)$, обозначим просто через q . Таким образом, $q = a_0\mathcal{H}(\mathfrak{M}, a_0, r, u)$. Из леммы 7 следует, что если r не меньше степени различимости автомата $\mathfrak{M}$, то автомат $\langle \mathfrak{M}', q \rangle$ является приведенным автоматом для автомата $\langle \mathfrak{M}, q \rangle$, и, следовательно,

$$T_{\langle \mathfrak{M}', q \rangle} = T_{\langle \mathfrak{M}, q \rangle} = T_{\langle \mathfrak{M}, a_0 \mathcal{H}(\mathfrak{M}, a_0, r, u) \rangle}.$$

Слова $\mathcal{G}(G, a_0, r, u)$ и $\mathcal{H}(\mathfrak{M}, a_0, r, u)$ у нас будут играть вспомогательную роль. Слово $\mathcal{H}(\mathfrak{M}, a_0, r, u)$ и, тем более, слово $\mathcal{G}(G, a_0, r, u)$ в общем случае не могут быть построены, используя только опрос автомата $\mathfrak{M}$: при построении слова $\mathcal{G}(G, a_0, r, u)$ требуется "заглянуть" в диаграмму автомата как при идентификации состояний типа p , так и при определении $g(G, p, r)\|\ell$; при построении слова $\mathcal{H}(\mathfrak{M}, a_0, r, u)$ также требуется "заглянуть" в диаграмму $\mathfrak{M}$, но только при идентификации состояний типа p (так как член $q_t = m(\mathfrak{M}, p_{s_{t-1}}, r)\|\ell$, согласно лемме 9, может быть эффективно найден, если мы знаем, как автомат $\langle \mathfrak{M}, p_{s_{t-1}} \rangle$ переработал предыдущие члены последовательности $m(\mathfrak{M}, p_{s_{t-1}}, r)$, а это мы можем восстановить по графу P , построенному в результате предыдущих шагов, и выходному слову, полученному в результате предыдущих шагов при подаче соответствующего начального куска слова $\mathcal{H}(\mathfrak{M}, a_0, r, u)$.

Определим теперь другое входное слово $\mathcal{M}(\mathfrak{M}, a_0, r, u)$. Это слово будет обладать тем дополнительным свойством, что его можно будет последовательно построить, используя только информацию о том, как автомат $\langle \mathfrak{M}, a_0 \rangle$ переработал предыдущий начальный кусок данного слова. Слово $\mathcal{M}(\mathfrak{M}, a_0, r, u)$ у нас будет являться основной составной частью при построении искомого эксперимента.

Слово $\mathcal{M}(\mathfrak{M}, a_0, r, u)$ определим в точности так же, как слово $\mathcal{H}(\mathfrak{M}, a_0, r, u)$, за исключением места, касающегося идентификации вершин типа p. А именно, идентификацию вершин типа p в автомате $\mathfrak{M}$ мы будем осуществлять, используя их характеристики. Более точно это означает следующее. При построении графа P каждой его вершине типа p мы будем приписывать ее характеристику: пусть p_j - некоторая вершина типа p автомата $\mathfrak{M}$ и $p_{(j)}$ - соответствующая вершина типа p графа P; пусть вершина p_j была получена из вершины q в результате подачи слова b', т.е. $p_j = qb'$ (q может быть как вершиной типа p, так и вершиной типа a); слово b' имеет вид $\underbrace{b(u)\, b(u) \dots b(u)}_{u^* \text{ раз}}$, и характеристика вершины p_j - это выходное слово (обозначим его через y), которое соответствует последнему $b(u)$-куску слова b', когда b' мы подаем начиная с q; тогда вершине $p_{(j)}$ графа P в момент, когда мы ее вводим в граф P, приписываем слово y, которое называем характеристикой данной вершины. Рассмотрим, например, шаг t процесса построения $\mathcal{M}(\mathfrak{M}, a_0, r, u)$. Пусть $p'_{(s'_{t-1})_t}$ - финальная вершина предыдущего шага. Тогда на шаге t, так же как и в случае $\mathcal{H}(\mathfrak{M}, a_0, r, u)$, сначала подаем слово $q_t = m(\mathfrak{M}, p_{s'_{t-1}}, r)\|\ell$, получаем вершину $a'_t = p_{s'_{t-1}}\, q'_t$, затем, начиная с a'_t, подаем слово b', получаем вершину $p_{j'_{t-1}} = a'_t b'$, добавляем к графу P вершину $p'_{(j'_{t-1})}$, помеченную характеристикой, и т.д., пока доходим до вершины $p'_{j'_t - 1}$ такой, что характеристика вершины $p'_{j'_{t-1}} b'$ совпадает с характеристикой некоторой из уже построенных вершин типа p графа P (пусть это будет вершина $p_{(r'_t)}$). В этом случае, как и раньше, из вершины $p_{(j'_{t-1})}$ в вершину $p_{(r'_t)}$ проводим ребро и помечаем его словом b'. Далее поступаем в точности так же, как при построении $\mathcal{K}(\mathfrak{M}, a_0, r, u)$. Финальную вершину шага t обозначаем через $p'_{(s'_t)}$.

Процесс построения слова $\mathcal{M}(\mathfrak{M}, a_0, r, u)$, так же как и процесс построения слова $\mathcal{K}(\mathfrak{M}, a_0, r, u)$, заканчивается на некоторой финальной вершине $q = a_0 \mathcal{M}(\mathfrak{M}, a_0, r, u)$, когда все слова последовательности $m(\mathfrak{M}, q, r)$ исчерпаны и построен автомат $\langle \mathfrak{M}', q \rangle$.

Из определения слова $\mathcal{M}(\mathfrak{M}, a_0, r, u)$ и леммы 9 непосредственно вытекает

ЛЕММА II. Для любого автомата $\langle \mathfrak{M}, a_0 \rangle$ и любых натуральных r и u слово $\mathcal{M}(\mathfrak{M}, a_0, r, u)$ и автомат $\langle \mathfrak{M}', q \rangle$ могут быть последовательно и эффективно построены, используя только то, как автомат $\langle \mathfrak{M}, a_0 \rangle$ перерабатывает предыдущий кусок слова $\mathcal{M}(\mathfrak{M}, a_0, r, u)$.

Пусть d - некоторое входное слово и $d' = \underbrace{dd \ldots d}_{u^6 \text{ раз}}$.
Пусть, далее, q_α - состояние автомата $\mathfrak{M}$ и q_α - характеристика состояния $q_\alpha d'$ -выходное слово, соответствующее последнему d-куску слова d', когда подача слова d' начинается с q_α (и, следовательно, кончается с $q_\alpha d'$). Будем говорить, что слово $d' = dd \ldots d$ правильно идентифицирует состояния $q_\alpha d'$ и $q_\beta d'$ автомата $\mathfrak{M}$, если истинно следующее утверждение: если q_α -характеристика состояния $q_\alpha d'$ совпадает с q_β -характеристикой состояния $q_\beta d'$, то $q_\alpha d'$ и $q_\beta d'$ неотличимы, и если $q_\alpha d'$ и $q_\beta d'$ совпадают, то q_α -характеристика состояния $q_\alpha d'$ совпадает с q_β-характеристикой состояния $q_\beta d'$.

Из изложенного выше следует, что если r не меньше степени различимости автомата $\mathfrak{M}$ и слово $b' = \underbrace{b(u) \ldots b(u)}_{u^6 \text{ раз}}$

в процессе построения $\mathcal{M}(\mathfrak{M}, a_0, r, u)$ правильно идентифицирует состояния автомата $\mathfrak{M}$, то слово $\mathcal{M}(\mathfrak{M}, a_0, r, u)$ задает простой эксперимент, который остаточно расшифровывает автомат $\langle \mathfrak{M}, a_0 \rangle$, т.е. строит автомат $\langle \mathfrak{M}', q \rangle$ такой, что $T_{\langle \mathfrak{M}', q \rangle} = T_{\langle \mathfrak{M}, a_0 \mathcal{M}(\mathfrak{M}, a_0, r, u) \rangle}$. Этот результат может быть обобщен еще следующим образом. Выше при построении слова $\mathcal{M}(\mathfrak{M}, a_0, r, u)$ и автомата $\langle \mathfrak{M}', q \rangle$ мы использовали слово $b' = \underbrace{b(u) \ldots b(u)}_{u^6}$. Обозначим через $\mathcal{M}(\mathfrak{M}, a_0, r, u, d)$ входное слово, которое строится в точности также, как слово $\mathcal{M}(\mathfrak{M}, a_0, r, u)$, только вместо слова $b' = \underbrace{b(u) \ldots b(u)}_{u^6}$ используется слово $d' = \underbrace{d \ldots d}_{u^6}$. Через $\langle \mathfrak{M}^d, q \rangle$ обозначим соответствующий автомат, который мы при этом получим (таким образом, если $d = b(u)$, то $\mathcal{M}(\mathfrak{M}, a_0, r, u) = \mathcal{M}(\mathfrak{M}, a_0, r, u, d)$ и $\langle \mathfrak{M}', q \rangle = \langle \mathfrak{M}^d, q \rangle$).

Еще заметим, что если слово d остаточно различает любые два состояния автомата $\langle \mathfrak{M}, a_0 \rangle$, достижимые из a_0, то слово $d' = \underbrace{d \ldots d}_{\kappa^2}$, где κ -верхняя оценка числа состояний, достижимых из a_0, правильно идентифицирует любые два состояния автомата $\langle \mathfrak{M}, a_0 \rangle$, достижимые из a_0. Поэтому имеет место

ЛЕММА 12. Если слово d остаточно различает любые два состояния автомата $\langle \mathfrak{M}, a_0 \rangle$, достижимые из a_0, r не меньше степени различимости множества состояний автомата $\langle \mathfrak{M}, a_0 \rangle$, достижимых из a_0, и κ - верхняя оценка числа состояний автомата $\langle \mathfrak{M}, a_0 \rangle$, достижимых из a_0, то слово $\mathcal{M}(\mathfrak{M}, a_0, r, \sqrt[3]{\kappa}, d)$ задает простой эксперимент, который расшифровывает автомат $\langle \mathfrak{M}, a_0 \rangle$, т.е. строит автомат $\langle \mathfrak{M}^d, q \rangle$ такой, что

$$T_{\langle \mathfrak{M}^d, q \rangle} = T_{\langle \mathfrak{M}, a_0 \mathcal{M}(\mathfrak{M}, a_0, r, \sqrt[3]{\kappa}, d) \rangle}$$

. В формулировке леммы 12 величина $\sqrt[3]{\kappa}$ возникает от того, что $d' = \underbrace{d \ldots d}_{\kappa^2} = \underbrace{d \ldots d}_{u^6}$: отсюда $u = \sqrt[3]{\kappa}$.

Оценим еще длину $\ell(\mathcal{M}(\mathfrak{M}, a_0, r, u))$ слова $\mathcal{M}(\mathfrak{M}, a_0, r, u)$. Общее число шагов, используемых при построении $\mathcal{M}(\mathfrak{M}, a_0, r, u)$, не превосходит $k \cdot km^{r+2}$, где k – число состояний автомата $\mathfrak{M}$, достижимых из a_0, а km^{r+2} – верхняя оценка числа членов последовательности $m(\mathfrak{M}, q_i, r)$ (см. (I) и (2)). Длина одного шага

$$\ell(\eta_t B' \dots B' z_t) = \ell(\eta_t) + \ell(B' \dots B') + \ell(z_t) \leqslant$$
$$\leqslant (k+r) + k\ell(B') + k(\max \ell(\eta_j) + \ell(B')) \leqslant$$
$$\leqslant (k+r) + k\ell(\underbrace{B(u) \dots B(u)}_{u^6}) + k(k+r) + k\ell(\underbrace{B(u) \dots B(u)}_{u^6}).$$

При $u \geqslant u''_\varepsilon$ (см. лемму 3) имеем $\ell(B(u)) < u^a$. Поэтому для таких u

$$\ell(\mathcal{M}(\mathfrak{M}, a_0, r, u)) \leqslant k^2 m^{r+2}((k+1)(k+r) + 2ku^{a+6}) \qquad (4)$$

Аналогично можно оценить длину $\ell(\mathcal{M}(\mathfrak{M}, a_0, r, u, d))$ слова $\mathcal{M}(\mathfrak{M}, a_0, r, u, d)$:

$$\ell(\mathcal{M}(\mathfrak{M}, a_0, r, u, d)) < km^{r+2}((k+1)(k+r) + 2ku^6 \ell(d).$$

Это означает, что длина эксперимента $\mathcal{M}(\mathfrak{M}, a_0, r, \sqrt[3]{k}, d)$ из леммы I2, остаточно расшифровывающего автомат $\langle \mathfrak{M}, a_0 \rangle$, удовлетворяет неравенству

$$\ell(\mathcal{M}(\mathfrak{M}, a_0, r, \sqrt[3]{k}, d)) \leqslant km^{r+2}((k+1)(k+r) + 2k^3 \ell(d)). \qquad (5)$$

Обозначим через $\mathcal{G}(G, a_0, r, u)_v$ (соответственно, через $\mathcal{H}(\mathfrak{M}, a_0, r, u)_v$ и $\mathcal{M}(\mathfrak{M}, a_0, r, u)_v$) минимальный начальный кусок x слова $\mathcal{G}(G, a_0, r, u)$ (соответственно, слов $\mathcal{H}(\mathfrak{M}, a_0, r, u)$ и $\mathcal{M}(\mathfrak{M}, a_0, r, u)$) такой, что на пути, начинающегося с вершины a_0 и задаваемым словом x, лежат v различных вершин графа G (автомата $\mathfrak{M}$); если на пути, начинающегося с вершины a_0 и задаваемым словом $\mathcal{G}(G, a_0, r, u)$ (соответственно, словами $\mathcal{H}(\mathfrak{M}, a_0, r, u)$ и $\mathcal{M}(\mathfrak{M}, a_0, r, u)$), лежит меньше чем v различных вершин, то положим $\mathcal{G}(G, a_0, r, u)_v = \mathcal{G}(G, a_0, r, u)$

(соответственно, $\mathcal{K}(\mathfrak{M}, a_0, r, u)_v =$
$= \mathcal{K}(\mathfrak{M}, a_0, r, u)$ и $\mathcal{M}(\mathfrak{M}, a_0, r, u)_v = \mathcal{M}(\mathfrak{M}, a_0, r, u)$).

Обозначим через $\mathcal{G}^*(G, a_0, r, u)_v$ (соответственно, через $\mathcal{K}^*(\mathfrak{M}, a_0, r, u)_v$ и $\mathcal{M}^*(\mathfrak{M}, a_0, r, u)_v$) множество вершин графа G (автомата $\mathfrak{M}$), лежащих на пути, начинающегося с вершины a_0 и задаваемым словом $\mathcal{G}(G, a_0, r, u)_v$ (соответственно, словами $\mathcal{K}(\mathfrak{M}, a_0, r, u)_v$ и $\mathcal{M}(\mathfrak{M}, a_0, r, u)_v$). Далее обозначим через $\mathcal{G}(G, a_0, r, u)_v^{-1}$ (соответственно, через $\mathcal{K}(\mathfrak{M}, a_0, r, u)_v^{-1}$) начальный кусок слова $\mathcal{G}(G, a_0, r, u)$ (слова $\mathcal{K}(\mathfrak{M}, a_0, r, u)$), который на одну букву короче слова $\mathcal{G}(G, a_0, r, u)_v$ (слова $\mathcal{K}(\mathfrak{M}, a_0, r, u)_v$).

ЛЕММА 13. Пусть u - натуральное число, U -подмножество вершин графа G такое, что $|U| \leq u^3$, $a_0 \in U$, $r(u) = 8 \log_n u$ и $\mathfrak{M}$ - автомат, принадлежащий $\tilde{G}$ и являющийся u -допустимым II и u-допустимым IV при U . Тогда для любого натурального v такого, что $\mathcal{G}^*(G, a_0, r, u)_v \subseteq U$ и $D\langle G, a_0 \mathcal{G}(G, a_0, r, u)_v^{-1}\rangle \geq 8 \log_n u$, имеет место

$$\mathcal{M}^*(\mathfrak{M}, a_0, r(u), u)_v = \mathcal{G}^*(G, a_0, r(u), u)_v .$$

ДОКАЗАТЕЛЬСТВО. Сначала докажем, что при условиях леммы

$$\mathcal{K}^*(\mathfrak{M}, a_0, r(u), u)_v = \mathcal{G}^*(G, a_0, r(u), u)_v .$$

Пусть l_1 и l_2 - два пути в графе G . Скажем, что l_1 содержится в l_2 , если вершины, содержащиеся в l_1 , содержатся также и в l_2 .

Скажем, что шаг t процесса построения $\mathcal{G}(G, a_0, r, u)$ является вторичным, если существует такое t' , $t' < t$, что шаги t и t' в процессе построения $\mathcal{G}(G, a_0, r, u)$ начинаются с одной и той же вершины $p_j = p_{s_{t-1}} = p_{s_{t'-1}}$, $p_j q_t = p_j q_{t'}$

и путь в графе G , начинающийся с вершины p_j и соответствующий слову q_t , содержится в пути, построенном в результате предыдущих шагов. О шаге t также будем говорить, что он похож на шаг t' . Скажем, что шаг t процесса построения $\mathcal{Y}(G, a_0, r, u)$ является несущественным, если он начинается и кончается на одной и той же вершине p и путь в графе G , построенный в результате этого шага (т.е. путь, начинающийся с p и соответствующий слову $q_t b'_1 \ldots b'_{z_t}$), содержится в пути, построенном в результате предыдущих шагов. Убедимся в справедливости следующего утверждения

С. Если шаг t процесса построения $\mathcal{Y}(G, a_0, r, u$ является вторичным, то он является также и несущественным.

Итак, пусть шаг t процесса построения $\mathcal{Y}(G, a_0, r, u)$ похож на некоторый шаг t' , $t'<t$ (т.е. $p_j = p_{s_{t-1}}$ и $p_j q_t = p_j q_{t'}$). На шаге t' , начиная с вершины p_j , мы подавали сначала $q_{t'}$, получили вершину $a_{t'} = p_j q_{t'}$, затем подавали слово b' , получили вершину $p_{j_{t'-1}} = a_{t'} b'$ и т.д.. На шаге t опять, начиная с вершины p_j , мы подаем q_t , получаем вершину $a_t = p_j q_t = p_j q_{t'} = a_{t'}$, затем подаем слово b' , получаем вершину $p_{j_{t-1}} = a_t b' = p_{j_{t'-1}}$ и т.д. Так как в процессе построения $\mathcal{Y}(G, a_0, r, u)$ шаги t' и t , $t'<t$, начинаются с одной и той же вершины p_j , то это означает, что путь в графе P , построенный в результате шагов $t', t'+1, \ldots, t-1$, представляет собой цикл:

$$p_{(j)}, a_{(t')}, p_{(j_{t'-1})}, \ldots, p_{(j)}.$$

Отсюда и из того, что $p_{(j_{t-1})} = p_{(j_{t'-1})}$, получаем, что в графе P из $p_{(j_{t-1})}$ ведет путь в $p_{(j)}$, причем вершина $p_{(j)}$ должна быть наиболее ранняя финальная вершина, в которую еще можно попасть из $p_{(j_{t-1})}$ (так как в противном случае вершина $p_{(j)}$ не была бы финальной вершиной шага $t-1$).
Это означает, что вершина p_j должна быть финальной вер-

шиной также и для шага t. Из изложенного выше также следует, что путь в графе G, построенный в результате шага t, содержится в пути, построенном в результате предыдущих шагов. Утверждение С доказано.

В доказываемой лемме речь идет только о начальном куске $\mathcal{Y}(G,a_0,r(u),u)_v$ слова $\mathcal{Y}(G,a_0,r(u),u)$. Так как согласно условиям леммы $\mathcal{Y}^*(G,a_0,r(u),u)_v \in U$, то, очевидно, для любой финальной вершины p_j, возникающей в процессе построения $\mathcal{Y}(G,a_0,r(u),u)_v$, в U будет содержаться также и $\tilde{g}^*(G,p_j,r(u))$; здесь $\tilde{g}(G,p_j,r(u))$ - начальный кусок последовательности $g(G,p_j,r(u))$, использованный в процессе построения $\mathcal{Y}(G,a_0,r(u),u)_v$ и $\tilde{g}^*(G,p_j,r(u))$, как и ранее, множество вершин, достижимых из p_j членами последовательности $\tilde{g}(G,p_j,r(u))$. Но в таком случае, согласно лемме 10, некоторый начальный кусок $\tilde{m}(\mathfrak{M},p_j,r(u))$ последовательности $m(\mathfrak{M},p_j,r(u))$ будет обладать тем свойством, что его можно будет получить из $\tilde{g}(G,p_j,r(u))$ вычеркиванием некоторых вторичных членов и добавлением некоторых новых вторичных членов. Это означает, учитывая доказанное выше утверждение С, что процесс построения начального куска $\mathcal{Y}(G,a_0,r(u),u)_v$ будет отличаться от процесса построения некоторого начального куска $\tilde{\mathcal{K}}(\mathfrak{M},a_0,r(u),u)$ слова $\mathcal{K}(\mathfrak{M},a_0,r(u),u)$ только тем, что некоторые несущественные шаги будут вычеркнуты и некоторые новые несущественные шаги будут добавлены. Но несущественные шаги не меняют множества вершин, достигнутых уже ранее. Поэтому $\mathcal{Y}^*(G,a_0,r(u),u)_v = \tilde{\mathcal{K}}(\mathfrak{M},a_0,r(u),u)$ и, следовательно, $\mathcal{Y}^*(G,a_0,r(u),u)_v = \mathcal{K}^*(\mathfrak{M},a_0,r(u),u)_v$.

Из условий леммы и только что доказанного равенства следует, что $\mathcal{K}^*(\mathfrak{M},a_0,r(u),u)_v \leq U$ и $D_{\langle G,a_0\mathcal{K}(\mathfrak{M},a_0,r(u),u)_v^{-1}\rangle} \geq 8\log_n u$. Отметим, забегая вперед, что дальнейшее рассуждение было бы более очевидным, если вместо условия $D_{\langle G,a_0\mathcal{K}(\mathfrak{M},a_0,r(u),u)_v^{-1}\rangle} \geq 8\log_n u$ было бы более сильное условие $D_{\langle G,a_0,\mathcal{K}(\mathfrak{M},a_0,r(u),u)_v\rangle} \geq 8\log_n u$.

Однако учитывая то, что построение $\mathcal{M}(\mathfrak{M}, a_0, r, u)$ проводится по кускам, где при построении очередного куска используются только то, как автомат переработал предыдущую часть слова $\mathcal{M}(\mathfrak{M}, a_0, r, u)$ (а не данный кусок[1]), нетрудно убедиться, что приведенное ниже рассуждение будет сохранять силу и при условии $D_{\langle G, a_0, \mathcal{H}(\mathfrak{M}, a_0, r(u), u)_v^{-1}\rangle} \geqslant 8\log_n u$. Состоит это рассуждение в следующем. Применяя лемму 4, получаем, что идентификация вершин типа p с помощью их характеристик, использованная в процессе построения $\mathcal{M}(\mathfrak{M}, a_0, r(u), u)_v$, дает в точности тот же самый результат, что и идентификация вершин по диаграмме автомата $\mathfrak{M}$, использованная в процессе построения $\mathcal{H}(\mathfrak{M}, a_0, r(u), u)_v$. Отсюда следует, что $\mathcal{M}^*(\mathfrak{M}, a_0, r(u), u)_v = \mathcal{H}^*(\mathfrak{M}, a_0, r(u), u)_v$ и, следовательно, учитывая доказанное выше равенство, $\mathcal{M}^*(\mathfrak{M}, a_0, r(u), u)_v = \mathcal{Y}^*(\mathfrak{M}, a_0, r(u), u)_v$. Лемма доказана.

Из леммы 13 легко вытекает

СЛЕДСТВИЕ. Пусть u - натуральное число, $r(u) = 8\log_n u$, U' - подмножество вершин графа G такое, что $|U'| \leqslant u$, $U = \bigcup_{q \in U'} \mathcal{Y}^*(G, q, r(u), u)_{u^2 - 8\log_n u}$ (следовательно, $|U| \leqslant u^3$) и $\mathfrak{M}$ - автомат, принадлежащий $\widetilde{G}$ и являющийся u-допустимым II и u-допустимым IV при U. Тогда для любой вершины $q \in U'$ слово $\mathcal{M}(\mathfrak{M}, q, r(u), u)$ обладает тем свойством, что для любого $v \leqslant u^2 - 8\log_n u$, если $D_{\langle \mathfrak{M}, q \mathcal{M}(\mathfrak{M}, q, r(u), u)_v\rangle} \geqslant 8\log_n u$, то $\mathcal{M}^*(\mathfrak{M}, q, r(u), u)_v = \mathcal{Y}^*(G, q, r(u), u)_v$.

В формулировке леммы 13 участвует условие $D_{\langle G, a_0 \mathcal{Y}(G, a_0, r(u), u)_v^{-1}\rangle} \geqslant 8\log_n u$. Мы теперь заменим лемму 13 другой леммой, в которой это условие уже не будет встречаться. Для этого обозначим через $\mathcal{D}_{\langle G, q\rangle}$ множество вершин, достижимых в графе G входными словами из вершины q (следовательно, $|\mathcal{D}_{\langle G, q\rangle}| = D_{\langle G, q\rangle}$), и положим

$$\mathcal{G}^*(G,a_0,r,u)_{v,s} = \begin{cases} \mathcal{G}^*(G,a_0,r,u)_v, & \text{если } D\langle G,a_0\,\mathcal{G}(G,a_0,r,u)_v\rangle \geq s, \\ \mathcal{G}^*(G,a_0,r,u)_v \cup \mathcal{D}\langle G,a_0\,\mathcal{G}(G,a_0,r,u)_v\rangle, & \text{если } D\langle G,a_0\,\mathcal{G}(G,a_0,r,u)_v\rangle < s \end{cases}$$

Очевидно, $|\mathcal{G}^*(G,a_0,r,u)_{v,s}| \leq v+s$. Из леммы I3 непосредственно вытекает

ЛЕММА I4. Пусть выполнены условия леммы I3, касающиеся u , U , a_0 , $r(u)$ и $\mathfrak{M}$. Тогда для любого натурального v такого, что $\mathcal{G}^*(G,a_0,r(u),u)_v \subseteq U$, имеет место $\mathcal{M}^*(\mathfrak{M},a_0,r(u),u)_v \subseteq \mathcal{G}^*(G,a_0,r(u),u)_{v,8\log_n u}$

Из леммы I4 вытекает

СЛЕДСТВИЕ. Пусть u - натуральное число, $r(u)=8\log_n u$, U' -подмножество вершин графа G такое, что $|U'| \leq u$, $U = \bigcup_{q\in U'} \mathcal{G}^*(G,q,r(u),u)_{u^2-8\log_n u,\,8\log_n u}$ (следовательно , $|U| \leq u^3$) и $\mathfrak{M}$ - автомат, принадлежащий $\widetilde{G}$ и являющийся u -допустимым П и u -допустимым IУ при U . Тогда для любой вершины $q \in U'$ слово $\mathcal{M}(\mathfrak{M},q,r(u),u)$ обладает тем свойством, что для любого $v \leq u^2-8\log_n u$ имеет место соотношение $\mathcal{M}^*(\mathfrak{M},q,r(u),u)_v \subseteq U.$

Теперь переходим к непосредственному построению искомого эксперимента. Искомый эксперимент у нас будет состоять из двух частей, которые назовем соответственно основной частью и заключительной частью. Пусть $\langle \mathfrak{M},q_0\rangle$ - произвольный автомат, к которому мы применяем этот эксперимент. Задача основной части эксперимента - найти некоторую верхнюю оценку числа состояний автомата $\mathfrak{M}$ (или, точнее, некоторую верхнюю оценку числа состояний автомата $\mathfrak{M}$, достижимых из того состояния, в которое он переходит в результате данной части эксперимента), а задача заключительной части - по верхней оценке числа состояний достаточно экономно расшифровать $\mathfrak{M}$.

Сначала определим основную часть эксперимента. Она будет состоять из отдельных шагов, следующих один за другим. В определении шага i, $i = 1, 2, \ldots$ будут встречаться обозначения $r(u)$, u_i, p_{i-1}. Положим

$$r(u) = 8 \log_n u;$$

$$u_1 = \max(u'_\varepsilon + 1,\ u''_\varepsilon + 1,\ u^{IV}_\varepsilon + 1{,}8);$$

где u'_ε, u''_ε, u^{IV}_ε - соответственно из леммы I, 3, 6;

$$u_i = u^3_{i-1} = u_1^{3^{i-1}},\quad i = 2, 3, \ldots;$$

$$p_0 = q_0,$$

где q_0 - начальное состояние экспериментируемого автомата;

$$p_{i-1},\qquad i = 2, 3, \ldots,$$

- будут определены индуктивно.

Шаг i ($i = 1, 2, \ldots$). Последовательно строим и подаем автомату $\langle \mathfrak{M}, p_{i-1} \rangle$ слово $\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i)$ и после подачи каждой буквы проверяем, существует ли автомат с менее чем u_i состояниями, который данный (начальный) кусок слова $\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i)$ перерабатывает так же, как автомат $\langle \mathfrak{M}, p_{i-1} \rangle$. Возможно одно из двух: либо после подачи автомату $\langle \mathfrak{M}, p_{i-1} \rangle$ некоторого начального куска $\mathcal{M}_i$ слова $\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i)$ (в частности, $\mathcal{M}_i$ может совпадать с $\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i)$) мы обнаружим, что $F_{\langle \mathfrak{M}, p_{i-1} \rangle}(\mathcal{M}_i) \geq u_i$, т.е. что невозможен автомат с менее чем u_i состояниями, который $\mathcal{M}_i$ перерабатывает так же, как $\langle \mathfrak{M}, p_{i-1} \rangle$, либо кончится слово $\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i)$. В обоих случаях заключительное состояние автомата $\langle \mathfrak{M}, p_{i-1} \rangle$ обозначим через p_i (в первом случае $p_i = p_{i-1}\mathcal{M}_i$, во втором случае $p_i = p_{i-1}\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i)$). Во втором случае основную часть эксперимента заканчиваем и переходим к заключительной части. В первом случае переходим к шагу $l+1$.

Таким образом, основная часть эксперимента будет продолжаться до такого шага i_0, когда впервые будет возможен автомат с менее чем u_{i_0} состояниями, который слово $\mathcal{M}(\mathfrak{M}, p_{i_0-1}, r(u_{i_0}), u_{i_0})$ (обозначим это слово через $\mathcal{M}_{i_0}$) перерабатывает так же, как автомат $\langle \mathfrak{M}, p_{i_0-1} \rangle$, т.е. $\bar{F}_{\langle \mathfrak{M}, p_{i_0-1} \rangle}(\mathcal{M}_{i_0}) < u_{i_0}$. Это означает, что основная часть искомого эксперимента представляет собой входное слово

$$\mathcal{M}_{\mathfrak{M}} = \mathcal{M}_1 \mathcal{M}_2 \ldots \mathcal{M}_{i_0}.$$

Пусть $|\mathfrak{M}| = \kappa$. Очевидно,

$$u_{i_0} \leqslant \max(u_1, \kappa^3). \qquad (6)$$

Так как $u_{i_0} = u_1^{3^{i_0-1}}$, то

$$i_0 \leqslant \log_3 \log_3 \max(u_1, \kappa^3) + 1.$$

Отсюда и из неравенства (4) получаем, что длина основной части эксперимента

$$l(\mathcal{M}_{\mathfrak{M}}) = \sum_{i=1}^{i_0} l(\mathcal{M}_i) \leqslant \sum_{i=1}^{i_0} l(\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i)) \leqslant \qquad (7)$$
$$\leqslant \sum_{i=1}^{i_0} \kappa^2 m^{r(u_i)+2} ((\kappa+1)(\kappa+r)(u_i)) + 2\kappa u_i^{a+6} \leqslant \kappa^{b} + b_\varepsilon,$$

где b - некоторая константа, не зависящая от κ и ε, и b_ε - константа, не зависящая от κ (но зависящая от ε).

Теперь покажем, что для достаточно большой доли автоматов $\mathfrak{M}$ из $\hat{G}$ описанная основная часть эксперимента удовлетворяет требуемым свойствам, т.е. позволяет найти верхнюю оценку числа состояний автомата $\mathfrak{M}$, достижимых из заключительного состояния. Для этого определим следующую систему подмножеств графа G:

$$U_0 = \{q_0\},$$
$$U_1 = \mathcal{Y}^+(G, q_0, r(u_1), u_1)_{u_1^2 - 8\log_n u_1,\, 8\log_n u_1},$$

$\vdots$

$$U_i = \bigcup_{q \in U_{i-1}} \mathcal{G}^*(G, q, r(u_i), u_i)_{u_i^2 - 8\log_n u_i,\ 8\log_n u_i},$$
$i = 2, 3, \ldots$

Таким образом,

$$|U_1| \leq u_1^3 = u_2, \quad |U_2| \leq u_2^3 = u_3, \ldots, |U_i| \leq u_i^3 = u_{i+1}, \ldots .$$

Пусть фиксировано подмножество U_i вершин графа G. Автомат $\mathfrak{M} \in \widetilde{G}$ назовем просто u_i -допустимым при U_i, если он является u_i -допустимым I, II, III, IV при U_i. Из условия $u_i \geqslant u_1 \geqslant \max(u_\varepsilon' + 1, u_\varepsilon'' + 1, u_\varepsilon''' + 1)$ и лемм I, 3, 5, 6 следует, что по крайней мере $(1 - 4\frac{\varepsilon}{u_i})$-ую долю из всех автоматов множества G составляют автоматы, являющиеся просто u_i - допустимыми при U_i. Автомат $\mathfrak{M} \in \widetilde{G}$ назовем глобально допустимым, если для любого $i = 1, 2, \ldots$ он является просто u_i -допустимым при U_i. Учитывая то, что $u_i = u_1^{3^{i-1}}$ и $u_1 = \max(u_\varepsilon' + 1, u_\varepsilon'' + 1, u_\varepsilon''' + 1, 8)$, получаем справедливость следующей леммы:

ЛЕММА I5. По крайней мере $(1 - \varepsilon)$ -ую долю из всех автоматов множества $\widetilde{G}$ составляют автоматы, являющиеся глобально допустимыми.

Теперь установим важную взаимосвязь между системой множеств U_i и основной частью эксперимента с автоматом $\mathfrak{M} \in \widetilde{G}$.

ЛЕММА I6. Если автомат $\mathfrak{M} \in \widetilde{G}$ является глобально допустимым и i_0 - номер последнего шага основной части эксперимента с $\mathfrak{M}$, то $p_{i_0} \in U_{i_0}$ и число состояний автомата $\mathfrak{M}$, достижимых из p_{i_0}, меньше чем $u_{i_0}^2$.

ДОКАЗАТЕЛЬСТВО. Будем говорить, что шаг i основной части эксперимента с $\mathfrak{M} \in \tilde{G}$ содержится в множестве U_i, если а) $p_{i-1} \in U_{i-1}$ и б) путь, соответствующий данному шагу (т.е. путь в графе G, начинающийся с p_{i-1} и определенный словом $\mathcal{M}_i$), содержится в U_i. Пусть $\mathfrak{M} \in \tilde{G}$ является глобально допустимым. Индукцией по i покажем, что для любого i шаг i содержится в U_i. Заметим, что $q_0 \in U_0$. Пусть теперь $p_{i-1} \in U_{i-1}$. Убедимся, что тогда шаг i содержится в U_i. Из следствия леммы I4 следует, что для любого $v \leq u_i^2 - 8 \log_n u_i$

$$\mathcal{M}^*(\mathfrak{M}, p_{i-1}, r(u_i), u_i)_v \subseteq U_i \qquad (8)$$

Далее, так как автомат $\mathfrak{M}$ является глобально допустимым, следовательно, также и u_i - допустимым I при U_i, то имеет место следующее: если при каком-нибудь начальном куске $\mathcal{M}'$ слова $\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i)$

$$|\mathcal{M}'^*| \geq u_i^2 - 8 \log_n u_i - 1,$$

то

$$\bar{F}_{\langle \mathfrak{M}, p_{i-1} \rangle}(\mathcal{M}') \geq u_i. \qquad (9)$$

Пусть шаг i не является последним. Согласно определению, он заканчивается, как только мы получаем начальный кусок $\mathcal{M}_i$ слова $\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i$ такой, что $\bar{F}_{\langle \mathfrak{M}, p_{i-1} \rangle}(\mathcal{M}_i) \geq u_i$ Отсюда (учитывая минимальность куска $\mathcal{M}_i$), согласно (9), получаем, что $|\mathcal{M}_i^*| \leq u_i^2 - 8 \log_n u_i - 1$ и, следовательно, $\mathcal{M}_i^* \subseteq$ $\subseteq \mathcal{M}^*(\mathfrak{M}, p_{i-1}, r(u_i), u_i)_{u_i^2 - 8 \log_n u_i - 1}$. Это означает, что $\mathcal{M}_i$ является начальным куском слова

$$\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i)_{u_i^2 - 8 \log_n u_i - 1}$$

Отсюда, согласно (8), получаем, что путь, соответствующий шагу i, содержится в U_i и, следовательно, сам шаг i тоже содержится в U_i. Пусть теперь шаг i является последним. Это означает, что

$$\bar{F}_{\langle \mathfrak{M}, p_{i-1} \rangle}(\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i)) < u_i.$$

Отсюда и из (9) получаем, что

$$\left|\mathcal{M}^*(\mathfrak{M}, p_{i-1}, r(u_i), u_i)_{u_i^2-8\log_n u_i-1}\right| < u_i^2-8\log_n u_i-1$$

и, следовательно,

$$\mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i)_{u_i^2-8\log_n u_i-1} = \mathcal{M}(\mathfrak{M}, p_{i-1}, r(u_i), u_i) = \mathcal{M}_i .$$

Отсюда по (8) опять получаем, что шаг i содержится в U_i. В частности, это означает, что $p_{i_0} \in U_{i_0}$, и тем самым первая часть леммы доказана.

Для доказательства второй части леммы предположим от противного, что $D_{\langle \mathfrak{M}, p_{i_0} \rangle} \geq u_{i_0}^2$. Из доказательства первой части леммы используем то, что $p_{i_0-1} \in U_{i_0-1}$ и число вершины v_0, достигнутых на последнем шаге, удовлетворяет неравенству $v_0 < u_{i_0}^2 - 8\log_n u_{i_0} - 1$. В таком случае для любой вершины q графа G, лежащей на пути, начинающегося с вершины p_{i_0-1} и определяемым словом $\mathcal{M}_{i_0} = \mathcal{M}(\mathfrak{M}, p_{i_0-1}, r(u_{i_0}), u_{i_0})$, имеем $D_{\langle G, q \rangle} \geq u_{i_0}^2 > 8\log_n u_{i_0}$. Отсюда, используя следствие леммы I3, получаем, что для любого $v < v_0 + 1 < u_{i_0}^2 - 8\log_n u_{i_0}$

$$\mathcal{M}^*(\mathfrak{M}, p_{i_0-1}, r(u_{i_0}), u_{i_0}) = \mathcal{G}^*(G, p_{i_0-1}, r(u_{i_0}), u_{i_0})_v \quad (10)$$

Но $\left|\mathcal{M}^*(\mathfrak{M}, p_{i_0-1}, r(u_{i_0}), u_{i_0})_{v_0+1}\right| = \left|\mathcal{M}^*(\mathfrak{M}, p_{i_0-1}, r(u_{i_0}), u_{i_0})_{v_0}\right| = v_0$.
Следовательно, $\left|\mathcal{G}^*(G, p_{i_0-1}, r(u_{i_0}), u_{i_0})_{v_0+1}\right| = v_0$. Это означает, что $\mathcal{G}^*(G, p_{i_0-1}, r(u_{i_0}), u_{i_0}) = \mathcal{M}_{i_0}^*$. Таким образом, путь, начинающийся с p_{i_0-1} и определяемый словом $\mathcal{G}(\mathfrak{M}, p_{i_0-1}, r(u_{i_0}), u_{i_0})$, содержит $v_0 < u_{i_0}^2 - 8\log_n u_{i_0} - 1$ вершин и заканчивается на вершине $p \in \mathcal{M}_{i_0}^*$. Но из любой вершины $p \in \mathcal{M}_{i_0}^*$ ведет путь в p_{i_0}. Поэтому из $D_{\langle G, p_{i_0} \rangle} \geq u_{i_0}^2$ следует $D_{\langle G, p \rangle} \geq u_{i_0}^2$. Но если это так, то словом $\mathcal{G}(G, p_{i_0}, r(u_{i_0}), u_{i_0})$ еще не достигнуты все вершины, которые вообще достижимы из p. Из определения слова $\mathcal{G}$ следует, что процесс его построения может заканчиваться только на такой вершине p, когда

все вершины, которые достижимы из ρ, уже достигнуты построенной частью слова $\mathcal{Y}$. Полученное противоречие доказывает нашу лемму.

Теперь опишем з а к л ю ч и т е л ь н у ю ч а с т ь искомого эксперимента. Пусть автомат $\mathfrak{M} \in \tilde{G}$ является глобально допустимым и i_0 - номер последнего шага основной части эксперимента. Рассмотрим число $u_{i_0+1} = u_{i_\gamma}^3$ и множество вершин U_{i_0+1}. Из леммы 16 и определения U_i, $i = i_0+1$, следует, что U_{i_0+1} обязательно будет содержать все вершины автомата $\mathfrak{M}$, которые достижимы из заключительного состояния ρ_{i_0}. Так как $\mathfrak{M}$ является глобально допустимым, то он является также и u_{i_0+1}-допустимым Ш и П при U_{i_0+1}. Это означает, во-первых, что степень различимости состояний, достижимых из ρ_{i_0}, не превосходит $7\log_n u_{i_0+1} + \log_n \frac{1}{\varepsilon}$, и во-вторых, что слово $b(u_{i_0+1})$, имеющее длину не более $u_{i_0+1}^a$, остаточно различает любые два состояния q_α, q_β, достижимые из ρ_{i_0}, если только хотя бы для одного из этих состояний (пусть это будет q_α) $D_{q_\alpha} b(u_{i_0+1}) \geqslant 8\log_n u_{i_0+1}$. Далее, согласно следствию леммы I из [2], для любого s эффективно можно построить безусловный простой эксперимент (входное слово) E_s длины не более $4ms(\ln ns)m^{2s}$, который остаточно расшифровывает любой автомат, имеющий не более чем s состояний. Это означает, в частности, что слово E_s остаточно различает любые два состояния q_α, q_β любого автомата $\mathfrak{A}$, если только число состояний, достижимых из q_α, и число состояний, достижимых из q_β, не превосходит s. Положим теперь

$$d = b(u_{i_0+1})\, E_s,$$

где $s = 8\log_n u_{i_0+1}$. Очевидно, $\ell(d) \leqslant u_{i_0+1}^{a'} + a''$.

Теперь заметим, что слово d остаточно различает любые два состояния q_α, q_β, достижимые из ρ_{i_0}. В самом деле, возможно только одно из двух: либо $(D_{q_\alpha} b(u_{i_0+1}) \geqslant 8\log_n u_{i_0+1}) \vee$

$\vee (D_{q_\beta} B(u_{i_0+1}) \geq 8 \log_n u_{i_0+1})$,

либо $(D_{q_\alpha} B(u_{i_0+1}) < 8 \log_n u_{i_0+1}) \& (D_{q_\beta} B(u_{i_0+1}) < 8 \log_n u_{i_0+1})$.

В первом случае слово $B(u_{i_0+1})$ должно остаточно различать q_α, q_β, и, следовательно, слово d тоже должно остаточно различать q_α, q_β. Во втором случае слово E_5 должно остаточно различать $q_\alpha B(u_{i_0+1})$, $q_\beta B(u_{i_0+1})$ и, следовательно, слово $d = B(u_{i_0+1}) E_5$ опять должно остаточно различать q_α, q_β. Таким образом, мы убедились, что если автомат $\langle \mathfrak{M}, q_0 \rangle \in \tilde{G}$ является глобально допустимым и i_0 – последний шаг основной части эксперимента с данным автоматом, то при $a_0 = p_{i_0}$, $d = B(u_{i_0+1}) E_5$, $r = 7 \log_n u_{i_0+1} + \log_n \frac{1}{\varepsilon}$ и $k = u_{i_0+1}$ выполняются предпосылки леммы 12. Отсюда по лемме 12 получаем, что слово $\mathcal{M}(\mathfrak{M}, p_{i_0}, r, \sqrt[3]{u_{i_0+1}}, d)$ (обозначаем его через $\tilde{\mathcal{M}}_{\mathfrak{M}}$) задает простой эксперимент, который расшифровывает автомат $\langle \mathfrak{M}, p_{i_0} \rangle$. Длина $l(\tilde{\mathcal{M}}_{\mathfrak{M}})$ этого эксперимента, согласно неравенству (5),

$$l(\tilde{\mathcal{M}}_{\mathfrak{M}}) \leq u_{i_0+1} m^{r+2} ((u_{i_0+1}+1)(u_{i_0+1}+r) + 2 u^3_{i_0+1} l(d)).$$

Отсюда, используя соотношения $u_{i_0+1} = u^3_{i_0}$, $r = 7 \log_n u_{i_0+1} + \log_n \frac{1}{\varepsilon}$ и $l(d) \leq u^{a'}_{i_0+1} + a''$, получаем

$$l(\tilde{\mathcal{M}}_{\mathfrak{M}}) \leq u^{g}_{i_0} + g_\varepsilon,$$

где g – константа, не зависящая от u_{i_0} и ε, g_ε – константа, не зависящая от u_{i_0}. Так как согласно неравенству (6) $u_{i_0} \leq \max(u_1, k^3)$, где $k = |\mathfrak{M}|$, то

$$l(\tilde{\mathcal{M}}_{\mathfrak{M}}) \leq k^{g'} + g'_\varepsilon. \tag{10}$$

Подчеркнем, что неравенство (10), так же как и неравенство (7), имеет место независимо от того, является ли автомат $\mathfrak{M}$ глобально допустимым или нет.

Этим описание заключительной части искомого эксперимента закончено. В заключение отметим только следующее. Учитывая лемму 12, легко видеть, что слово $\tilde{\mathcal{M}}_{\mathfrak{M}}$ (так же как и слово $\mathcal{M}_{\mathfrak{M}}$, соответствующее основной части эксперимента) может быть последовательно и эффективно построено, используя только то, как автомат $\mathfrak{M}$ перерабатывает предыдущий кусок данного слова.

Теперь искомый эксперимент E над $\mathfrak{M}$ определим как конкатенацию

$$\mathcal{M}_{\mathfrak{M}}\,\tilde{\mathcal{M}}_{\mathfrak{M}}.$$

Из неравенств (7) и (10) следует, что длина этого эксперимента

$$E^*(\mathfrak{M}) = \ell(\mathcal{M}_{\mathfrak{M}}\,\tilde{\mathcal{M}}_{\mathfrak{M}}) < |\mathfrak{M}|^c + C_\varepsilon,$$

где c - константа, не зависящая от $\mathfrak{M}$ и ε, C_ε - константа, не зависящая от $\mathfrak{M}$.

Пусть автомат $\mathfrak{M}$ является глобально допустимым. Тогда согласно изложенному выше, эксперимент, соответствующий слову $\tilde{\mathcal{M}}_{\mathfrak{M}}$, расшифровывает автомат $\langle \mathfrak{M}, p_{i_0} \rangle = \langle \mathfrak{M}, q_0\mathcal{M}_{\mathfrak{M}}$ Но это означает, что эксперимент E, соответствующий конкатенации $\mathcal{M}_{\mathfrak{M}}\,\tilde{\mathcal{M}}_{\mathfrak{M}}$ расшифровывает сам автомат $\langle \mathfrak{M}, q_0 \rangle$. Согласно лемме 15, по крайней мере $(1-\varepsilon)$ -ую долю из всех автоматов множества $\tilde{\mathfrak{G}}$ составляют автоматы, являющиеся глобально допустимыми. Отсюда следует справедливость нашей теоремы.

Открытым остается вопрос о том, можно ли получить аналогичную оценку длины эксперимента в случае итеративных алгоритмов расшифровки (определение см. в [1]).

ЛИТЕРАТУРА

1. Трахтенброт Б.А., Барздинь Я.М. Конечные автоматы (поведение и синтез). М., 1970.
2. Барздинь Я.М. О расшифровке автоматов при отсутствии верхней оценки числа состояний.- ДАН СССР, 1970, т. 190, № 5.

ПОСТРОЕНИЕ ПОЛНЫХ СИСТЕМ ПРИМЕРОВ ДЛЯ ПРОГРАММ, РАБОТАЮЩИХ С ПРЯМЫМ МЕТОДОМ ДОСТУПА

Я.М.Барздинь, А.А.Калниньш

В работе [I] было рассмотрено построение полных систем примеров при последовательном методе доступа. В настоящей работе рассматривается задача построения полных систем примеров, когда наряду с последовательным методом доступа для массивов (файлов) используется также и прямой метод доступа. Прямой метод доступа характеризуется тем, что данные можно выбирать из масива непосредственно по их адресам или ключам.

Для формализации существенной части этой задачи по аналогии с [I] введем некоторую абстрактную машину, работающую с массивами (файлами). Эта машина будет использовать (в отличие от [I]) два способа доступа - последовательный и прямой. Массивы последовательного доступа (также как в [I]) будем считать расположенными на лентах, а массивы прямого доступа - на носителях другого типа, называемых дисками. Формально диски можно представить себе так же как ленты, ячейки которых перенумерованы числами ...,-2,-I,0,I,2,3,...*). Разница будет состоять в командах, которые будут допускаться для лент и для дисков.

---

*) Можно также считать, что ячейки перенумерованы числами I,2,3,...; от этого дальнейшие результаты не меняются, только в доказательствах добавляются некоторые дополнительные неравенства.

Кроме того, наша машина, так же как в [I], содержит конечное число внутренних ячеек a, b, ..., v. Далее, как ленты, так и диски разделены на входные и выходные. Произвольную входную (выходную) ленту обозначим через X (соответственно Y), а произвольный входной (выходной) диск - через $\varkappa$ (соответственно λ). На рис.I изображен схематический вид такой машины.

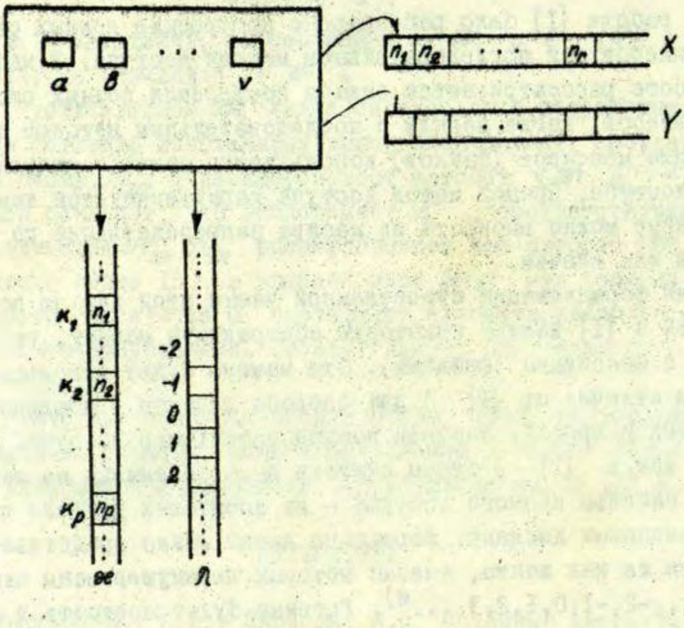


Рис. I.

Под массивом последовательного доступа будем понимать конечную последовательность целых чисел. Будем говорить, что на ленте записан массив $(n_1, n_2, \dots, n_r)$, если начиная с первой ячейки записаны числа $n_1, n_2, \dots, n_r$, а остальные ячейки пустые[ж)] (рис.1). Числа $n_1, n_2, \ldots, n_r$, следуя традиции, будем называть записями массива. i-ю запись массива X будем обозначать через X_i.

Под массивом прямого доступа будем понимать последовательность пар целых чисел. Будем говорить, что на диске записан массив $(\kappa_1,n_1), (\kappa_2,n_2),\ldots,(\kappa_p,n_p)$, если в κ_i-ой ячейке записано число n_i, $i=1,2,\ldots,p$, а остальные ячейки пустые (рис.1). Числа $n_1, n_2, \ldots$ будем называть записями массива, а $\kappa_1, \kappa_2 \ldots$ – ключами (или адресами) соответствующих записей. Запись n_i массива æ с ключом κ_i будем обозначать через $\text{æ}(\kappa_i)$ или æ_{κ_i}.

В дальнейшем, говоря о массиве X (массиве æ), будем понимать массив, записанный на ленте X (диске æ).

Определим теперь команды, которые может выполнить машина. Первые шесть из них в точности совпадают с соответствующими командами из [1]:

1) $X \Longrightarrow t$ – содержимое обозреваемой ячейки ленты X переписывается во внутреннюю ячейку t (т.е. ячейке t присваивается очередная запись массива X) и головка передвигается на одну ячейку вправо. Команда имеет два выхода: выход "+", когда обозреваемая ячейка содержит число, выход "-", когда обозреваемая ячейка пустая. В последнем случае значение ячейки t не меняется;

2) $t \Longrightarrow Y$ – содержимое внутренней ячейки t переписывается в обозреваемую ячейку ленты Y, а головка передвигается на одну ячейку вправо. Команда имеет один выход, который для определенности обозначим через "+";

3) $t \Longrightarrow u$ $(c \Longrightarrow u)$ – содержимое ячейки t (или константа c) переписывается в ячейку u. Команда имеет один выход, который также обозначим через "+";

ж) Содержимое (значение) пустой ячейки будем обозначать через φ. Будем считать, что φ меньше любого целого числа.

4) $t < u$ $(c < u,\ t < c)$ – команда имеет два выхода: если содержимое ячейки t (константа c) меньше содержимого ячейки u (или константы c), то управление передается по выходу "+", в противном случае по выходу "-";

5) НОП – ничего не делается (нет операции); команда имеет один выход "+";

6) СТОП – машина останавливается, команда не имеет выходов.

Специфическими для прямого метода доступа являются следующие две команды:

7) $\varkappa(t) \Longrightarrow u$ $(\varkappa(c) \Longrightarrow u)$ – для диска $\varkappa$ содержимое ячейки с номером, равным содержимому внутренней ячейки t (или равным константе c), переписывается во внутреннюю ячейку u . Команда имеет два выхода: выход "+", когда ячейка $\varkappa(t)$ содержит число, выход "-", когда ячейка пустая;

8) $u \Longrightarrow \lambda(t)$ $(u \Longrightarrow \lambda(c))$ – содержимое внутренней ячейки u переписывается в ячейку диска λ с номером, равным содержимому внутренней ячейки t (или равным константе c). Команда имеет один выход "+".

Под п р о г р а м м о й, работающей с п р я м ы м м е т о д о м д о с т у п а, мы будем понимать программу, записанную в указанной системе команд. Программы мы будем изображать в виде граф-схем.

На рис. 2 изображен пример программы корректировки массива X в зависимости от информации, записанной в массиве прямого доступа $\varkappa$. Массив X имеет вид

$$a_1, n_1^1, \ldots, n_{r_1}^1, 0, a_2, n_1^2, \ldots, n_{r_2}^2, \ldots \ldots, 0, a_k, n_1^k, \ldots, n_{r_k}^k.$$

Записи $n_1^i, \ldots, n_{r_i}^i$ можно интерпретировать как фамилии людей (закодированные в виде чисел), а a_i – как признак, указывающий, что надо делать с последующим набором фамилий. Выходной массив Y имеет аналогичный вид

$$a_1, n_{\alpha_1}^1, \ldots, n_{\alpha_e}^1, 0, a_2, n_{\beta_1}^2, \ldots, n_{\beta_f}^2, \ldots \ldots 0, a_k, n_{\varepsilon_1}^k, \ldots, n_{\varepsilon_h}^k,$$

где $n^i_{\nu_1}, \ldots, n^i_{\nu_g}$ - подпоследовательность последовательности $n^i_1, \ldots, n^i_{r_i}$, которая получается, если выделить те n^i_j, для которых $æ(n_j^i) < a_i$. Таким образом, массив $æ$ можно представить себе как справочник, где относительно каждой фамилии (рассматриваемой как ключ) указан определенный признак (число) и для каждого набора $(a_i, n^i_1, \ldots, n^i_{r_i})$ входного массива требуется выделить те фамилии, относительно которых в массиве $æ$ указан признак, меньший a_i. Программа, изображенная на рис.2, написана ошибочно: в выходном массиве Y она пропускает нули между наборами $(a_1, n^1_{\alpha_1}, \ldots, n^1_{\alpha_e}), (a_2, n^2_{\beta_1}, \ldots, n^2_{\beta_f}), \ldots$

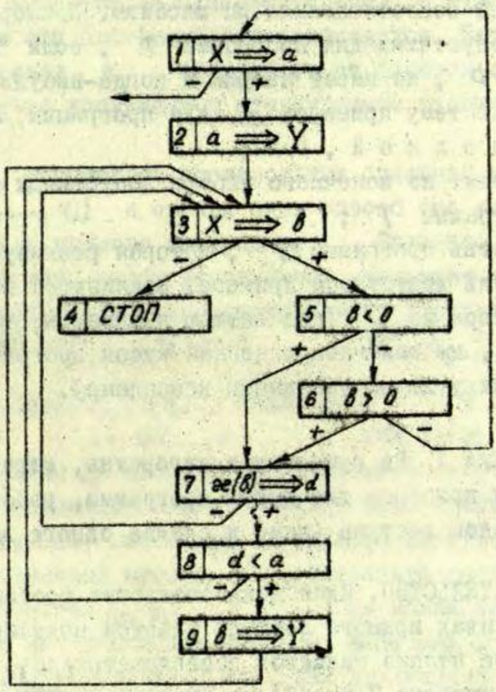


Рис. 2.

При построении граф-схемы программы допускается, что выходы некоторых команд остаются свободными. Выполнение программы начинается с первой команды. Предполагается, что в момент запуска программы все внутренние ячейки содержат нули. Программа останавливается, когда она попадает на команду СТОП. В случае, когда программа попадает на свободный выход, будем считать, что с ней происходит авария.

Под примером P мы будем понимать сопоставление, которое каждой входной ленте и каждому входному диску ставит в соответствие конкретный массив. Под применением программы T к примеру P будем понимать выполнение программы T при условии, что на входных лентах и дисках записаны сопоставленные им массивы. Пример P будем называть допустимым для программы T, если T, примененная к P, не имеет аварий и когда-нибудь останавливается. Систему примеров $\sum$ для программы T будем называть полной, если:

1) $\sum$ состоит из конечного набора допустимых примеров для программы T;
2) любая ветвь программы T, которая реализуема на каком-нибудь допустимом примере, реализуема на некотором примере из $\sum$ (под ветвью программы, так же как в [I], мы понимаем линейный кусок программы, лежащей между двумя условными командами).

ТЕОРЕМА I. **Не существует алгоритма, строящего полную систему примеров для любой программы, работающей с прямым методом доступа (даже в случае одного диска).**

ДОКАЗАТЕЛЬСТВО. Идея доказательства состоит в том, что на массивах прямого доступа удается моделировать многократное чтение массивов последовательного доступа. А согласно теореме 7 из [2] не существует алгоритма, строящего полную систему примеров для программ, использующих многократное (даже двукратное) чтение одних и тех же входных массивов, при этом достаточно ограничиться только двумя входными лентами. Фактически для доказательства теоремы нам понадобится несколько более сильное утверждение, вытекающее непосредственно из доказательства теоремы 7 [2] . Для его формулировки рассмотрим программы в системе команд K_4 (см. [2]), использующие только две входные ленты X и Z . Массив (следовательно и набор массивов - пример) будем называть бинарным, если записи принимают только два значения: 0 или 1 . Тогда невозможен алгоритм, с помощью которого для любой программы указанного вида в системе команд K_4 можно было определить, существует ли бинарный пример $P^0=(X^0, Z^0)$, на котором эта программа останавливается. Напомним, что система команд K_4 отличается от базовой системы команд тем, что допускается многократное чтение входных массивов.

Итак, рассмотрим произвольный бинарный массив $X=(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r)$ и опишем один способ его изображения в виде массива прямого доступа $æ$. Элементы массива $æ$ определены так, чтобы выполнялось следующее свойство: если мы рассмотрим последовательность элементов

$$s_0 \overset{df}{=} æ(1), \quad s_1 \overset{df}{=} æ(s_0), \dots, \quad s_i \overset{df}{=} æ(s_{i-1}), \dots,$$

то должно быть $s_{i-1} > s_i$, если $\varepsilon_i = 1$ и $s_{i-1} < s_i$, если $\varepsilon_i = 0$, $i = 1, 2, \dots, r$, $æ(s_r) = \varphi$. Таким образом, элементы ε_i массива X закодированы в массиве $æ$ с помощью отношений $>$ и $<$ между элементами s_{i-1} и s_i . Обратно, любой массив прямого доступа $æ$ задает один единственный массив X . Указанную последовательность элементов $s_0, s_1, \dots, s_i, \dots$ мы можем легко выделить из массива $æ$ с помощью команды $æ(t) \Longrightarrow u$. Для этого нужна только константа $c=1$ для извлечения первого элемента s_0 . Такую константу мы можем предварительно заслать в некоторую внутреннюю ячейку и держать там неограниченно долго и тем самым осуществить многократное выделение последовательности $s_0, s_1, \dots, s_i, \dots$. Отсюда следует, что с помощью нашей системы команд по массиву $\varkappa$ мы можем последовательно дешифровать элементы массива X , при этом такую процедуру мы можем осуществить многократно. Это означает, что если вместо массива X задать его изображение в виде массива $\varkappa$, то тем самым с помощью наших команд мы сможем моделировать многократное чтение массива X и, вообще, всю работу программы в системе команд K_4 , работающую с массивом X . Легко видеть, что указанное моделирование возможно с такой точностью, что моделирующая программа останавливается на тех и только тех массивах $\varkappa$, для которых, если вместо $\varkappa$ брать соответствующий X , останавливается моделируемая программа. Если существовал бы алгоритм, с помощью которого для любой программы мы могли бы построить полную систему примеров, то существовал и алгоритм, с помощью которого для любой программы могли определить, существует ли пример, на котором программа останавливается. Отсюда следует справедливость теоремы I. (Заметим, что несколько модифицируя описанный способ кодировки массивов, можно получить нужную нам кодировку двух массивов последовательного доступа на одном массиве прямого доступа. Отсюда следует неразрешимость указанной проблемы также и в случае одного диска.)

Рассмотрим теперь одно весьма общее с практической точки зрения достаточное условие, при котором проблема построения полной системы примеров для программ, работающих с прямым методом доступа, еще оказывается разрешимой.

Пусть $\alpha=(K_1, K_2, \dots, K_r)$ - произвольный путь в программе, K_i - команда с фиксированным выходом (+ или -). Например, $\alpha=(X \Rightarrow a+,\ a \Rightarrow Y+,\ X \Rightarrow b+,\ b<0-,\ b>0+,\ \varkappa(b) \Rightarrow d+,\ d<a-)$ (см. рис. 2). В дальнейшем будем счи-

тать, что п у т ь всегда начинается с первой команды.

Пусть произвольным образом фиксированы входные массивы и пусть $\text{æ}^{(1)}, \ldots, \text{æ}^{(s)}$ - входные массивы прямого доступа, используемые в данной программе. В таком случае после выполнения каждой команды пути внутренние ячейки принимают определенные значения (имеется в виду содержимое этих ячеек).

Будем рассматривать подпоследовательности

$$(K_{m_1}, K_{m_2}, \ldots, K_{m_p})$$

пути α, которые при заданной фиксации входных массивов обладают свойством:

K_{m_1} имеет вид $\text{æ}^{(\delta_1)}(\mu_1) \Rightarrow \cdots +, \delta_1 \in \{1, \ldots, s\}$,

K_{m_2} имеет вид $\text{æ}^{(\delta_2)}(\mu_2) \Rightarrow \cdots +$, где[*] $\mu_2 = \text{æ}^{(\delta_1)}(\mu_1)$, $\delta_2 \in \{1, \ldots, s\}$,

K_{m_3} имеет вид $\text{æ}^{(\delta_3)}(\mu_3) \Rightarrow \cdots +$, где $\mu_3 = \text{æ}^{(\delta_2)}(\mu_2)$, $\delta_3 \in \{1, \ldots, s\}$,

- -

K_{m_p} имеет вид $\text{æ}^{(\delta_p)}(\mu_p) \Rightarrow \cdots +$, где $\mu_p = \text{æ}^{(\delta_{p-1})}(\mu_{p-1})$, $\delta_p \in \{1, \ldots, s\}$.

Под степенью инцидентности пути α будем понимать наибольшую длину таких цепочек $(K_{m_1}, K_{m_2}, \ldots, K_{m_p})$, которые обладают указанным свойством при любой фиксации входных массивов, реализующих путь α. С т е п е н ь и н ц и д е н т н о с т и п р о г р а м м ы - максимальная степень инцидентностей путей программы.

ТЕОРЕМА 2. Существует алгоритм, который для любой программы, работающей с прямым методом доступа и имеющий ограниченную степень инцидентности, строит полную систему примеров.

---

[*] Равенство $\mu_2 = \text{æ}^{(\delta_1)}(\mu_1)$ более точно означает следующее: $\bar{\mu}_2 = \text{æ}^{(\delta_1)}(\bar{\mu}_1)$, где $\bar{\mu}_1$ - значение ячейки μ_1 в момент выполнения команды K_{m_1}, $\bar{\mu}_2$ - значение ячейки μ_2 в момент выполнения команды K_{m_2}. Аналогично понимаются и дальнейшие равенства.

ДОКАЗАТЕЛЬСТВО. Для простоты будем считать, что у нас имеется только один массив X последовательного доступа и только один массив $\mathfrak{X}$ прямого доступа. Приведенное нами доказательство непосредственно переносится также и на случай нескольких массивов; усложняются только обозначения. Через t и u обозначим произвольные внутренние ячейки. Пусть $\alpha=(K_1, K_2,\dots, K_r)$ - произвольный путь в программе. Сопоставим этому пути определенную систему неравенств $N(\alpha)$:

$$N(\alpha)=\begin{cases}\mathfrak{M}_1\\ \mathfrak{M}_2\\ \vdots\\ \mathfrak{M}_r\end{cases},$$

где $\mathfrak{M}_i$ - подсистема неравенств, соответствующая команде K_i. А именно, пусть t_k и u_ℓ - переменные, обозначающие соответственно значения (содержимое) внутренних ячеек t и u после прохождения пути $\alpha_i=(K_1,\dots,K_{i-1})$ и X_s - последняя запись, считанная с массива X за это время (в начальный момент эти переменные соответственно t_0, u_0, x_0). Пусть c - обозначение константы (произвольным образом фиксированного целого числа). Определим теперь систему $\mathfrak{M}_i$:

I) Если команда K_i имеет вид $X\Rightarrow u-$, то

$$\mathfrak{M}_i=\begin{cases}X_{s+1}<\varphi.\end{cases}$$

2) Если команда K_i имеет вид $X\Rightarrow u+$ и среди $\mathfrak{M}_1, \mathfrak{M}_2,\dots$ $\dots, \mathfrak{M}_{i-1}$ не встречаются неравенства вида $X_j<\varphi$ для некоторого j (т.е. раньше не встречаются команды вида $X\Rightarrow\dots-$), то

$$\mathfrak{M}_i=\begin{cases}X_{s+1}>\varphi\\ X_{s+1}=u_{\ell+1}\end{cases}$$

:

Заметим, что в данном случае вводятся новые переменные $u_{\ell+1}$ и X_{s+1}, которые для команды K_{i+1} будут играть такую же роль, как u_ℓ и X_s для команды K_i.

Если же раньше встречается неравенство вида $X_j < \varphi$, то

$$\mathfrak{M}_i = \begin{cases} X_{s+1} < \varphi \\ X_{s+1} > \varphi, \end{cases}$$

т.е. в качестве $\mathfrak{M}_i$ выбирается явно противоречивая система.

3) Если команда K_i имеет вид $t \Longrightarrow u$ (или $c \Longrightarrow u$), то

$$\mathfrak{M}_i = \{ t_\kappa = u_{\ell+1} \text{ (или } \mathfrak{M}_i = \{ c = u_{\ell+1} \text{)}.$$

В данном случае опять вводится новая переменная $u_{\ell+1}$.

4) Если команда K_i имеет вид $t < u +$ (или $c < u +$, или $t < c +$), то

$$\mathfrak{M}_i = \{ t_\kappa < u_\ell \text{ (или } \mathfrak{M}_i = \{ c < u_\ell \text{ , или } \mathfrak{M}_i = \{ t_\kappa < c \text{)}.$$

5) Если команда K_i имеет вид $t < u -$ (или $c < u -$, или $t < c -$), то

$$\mathfrak{M}_i = \{ t_\kappa > u_\ell \text{ (или } \mathfrak{M}_i = \{ c > u_\ell \text{ , или } \mathfrak{M}_i = \{ t_\kappa > c \text{)}.$$

6) Если команда K_i имеет вид $\text{æ}(t) \Longrightarrow u-$ (или $\text{æ}(c) \Longrightarrow u-$), то

$$\mathfrak{M}_i = \{ \text{æ}_{t_\kappa} < \varphi \quad \text{ (или } \mathfrak{M}_i = \{ \text{æ}_c < \varphi \text{)}.$$

7) Если команда K_i имеет вид $\text{æ}(t) \Longrightarrow u+$ (или $\text{æ}(c) \Longrightarrow u+$), то

$$\mathfrak{M}_i = \begin{cases} \text{æ}_{t_\kappa} > \varphi \\ \text{æ}_{t_\kappa} = u_{\ell+1} \end{cases} \qquad \left(\text{или } \mathfrak{M}_i = \begin{cases} \text{æ}_c > \varphi \\ \text{æ}_c = u_{\ell+1} \end{cases} \right).$$

В последних двух случаях вводится новая переменная вида æ_{t_k}. Такие переменные мы в дальнейшем будем называть д в о й н ы м и, так как, с одной стороны, переменной является сам индекс t_k, а с другой стороны, переменной (другой) является также и само æ_{t_k}. (Подчеркнем, что переменные вида æ_c, где c – константа, мы не будем называть двойными переменными.)

Рассмотрим пример. Пусть

$$\alpha = (X \Rightarrow a+,\ a \Rightarrow Y+,\ X \Rightarrow b+,\ b < 0-,\ b > 0+,\ \text{æ}(b) \Rightarrow d+,\ d < a-,\ X \Rightarrow b+,\ b < 0+$$

В этом случае

$$N(\alpha) = \left\{ \begin{array}{ll} x_1 > \varphi & \rbrace\ X \Rightarrow a+ \\ x_1 = a_1 & \\ & \rbrace\ a \Rightarrow Y+ \\ x_2 > \varphi & \rbrace\ X \Rightarrow b+ \\ x_2 = b_1 & \\ b_1 \geq 0 & \rbrace\ b < 0- \\ b_1 > 0 & \rbrace\ b > 0+ \\ \text{æ}_{b_1} > 0 & \rbrace\ \text{æ}(b) \Rightarrow d+ \\ \text{æ}_{b_1} = d_1 & \\ d_1 \geq a_1 & \rbrace\ d < a- \\ x_3 > \varphi & \rbrace\ x \Rightarrow b+ \\ x_3 = b_2 & \\ b_2 < 0 & \rbrace\ b < 0+ \end{array} \right.$$

Из приведенного определения $N(\alpha)$ следует, что ее переменными являются буквы $X, \text{æ}, \ldots, t, u, \ldots$ с индексами, притом индекс буквы æ в свою очередь может быть переменной. Это следует учесть при определении решения системы $N(\alpha)$: если значение t_k равно значению u_ℓ, то значение æ_{t_k} тоже должно быть равно значению æ_{u_ℓ}. Под решением системы $N(\alpha)$ мы понимаем любой набор ц е л о ч и с л е н н ы х значений переменных, удовлетворяющих данной системе.

В приведенном выше примере система $N(\alpha)$ имеет, например, следующее решение:

$$x_1 = a_1 = 1, \quad x_2 = b_2 = 2, \quad \varkappa_2 = 4, \quad x_3 = b_2 = -1.$$

Вообще система $N(\alpha)$ может иметь много решений. В дальнейшем, говоря о совокупности решений, мы будем иметь в виду совокупность в с е х решений системы $N(\alpha)$.

Далее, мы говорим, что путь α реализуем, если существует пример, на котором программа проходит (реализует) этот путь. Из определения системы $N(\alpha)$ непосредственно вытекает

ЛЕММА I. Путь α реализуем тогда и только тогда, когда система неравенств $N(\alpha)$ имеет решение. При этом для любого решения, если из него выделить значения переменных вида $x_1, x_2, \dots, \dots, \varkappa_{-1}, \varkappa_0, \varkappa_1, \varkappa_2, \dots,$ то они образуют пример, реализующий путь α .

Иногда нам будет удобно систему неравенств $N(\alpha)$ и ей подобные системы N изобразить в виде графа GN . Сначала определим граф $G'N'$. Его вершинами являются переменные и константы (в том числе и Φ), входящие в N (каждому двойному переменному также соответствует одна вершина). Неравенство $\zeta < \xi$ мы будем изображать в виде дуги (ξ, ζ) , которой приписан вес 1 , неравенство $\zeta \leqslant \xi$ - в виде дуги (ξ, ζ) , которой приписан вес 0 , а равенство $\zeta = \xi$ - как $\zeta \leqslant \xi$ и $\xi \leqslant \zeta$. На рис.4 изображен $G'N(\alpha)$, соответствующий предыдущему примеру. Далее, для того, чтобы из $G'N$ получить GN, делаем следующее: с двойных переменных $\varkappa_p$ стираем переменный индекс p и вместо этого из вершины, соответствующей $\varkappa_p$, проводим прерывистую стрелочку в вершину p (в случае системы $N(\alpha)$ и в других рассматриваемых нами случаях, такая вершина p

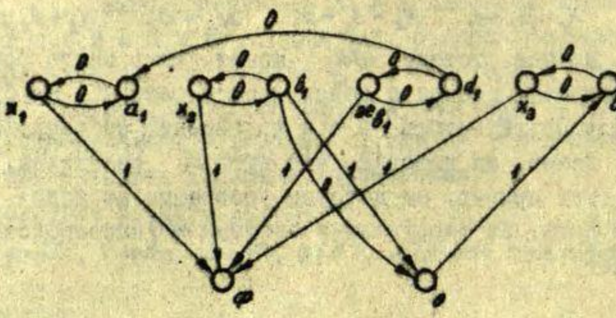


Рис. 4.

обязательно существует). На рис.5 изображен $GN(\alpha)$ соответствующий $G'N(\alpha)$ из рис.4.

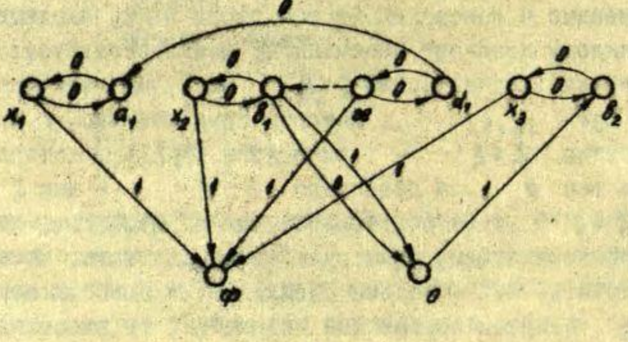


Рис. 5.

Очевидно, по GN однозначно можно восстановить индексы двойных переменных и, тем самым, систему неравенств N.

Теперь естественным образом можно определить равенство двух вершин ζ, ξ (переменных или констант) графа GN :

1) $\zeta = \xi$, если $\zeta \leqslant \xi$ и $\xi \geqslant \zeta$;
2) $\zeta \leqslant \xi$, если $\zeta \leqslant \xi$;
3) $\zeta < \xi$, если существует вершина η такая, что $\zeta \leqslant \eta$ и $\eta < \xi$;
4) $\zeta = \xi$, если существует вершина η такая, что $\zeta = \eta$ и $\eta = \xi$;
5) $\varkappa_\zeta = \varkappa_\xi$, если $\zeta = \xi$.

Определенное выше понятие равенства, там где это может вызывать недоразумения, мы будем называть синтаксическим равенством. Очевидно, оно несколько слабее фактического равенства, так как, например, в случае системы

$$\begin{cases} 4 < \zeta < 6 \\ 4 < \xi < 6 \end{cases}$$

переменные ζ и ξ фактически являются равными, однако согласно приведенному выше определению равенства эти переменные не будут равными.

Наряду с синтаксическим равенством можно ввести также и другое понятие равенства: переменные ζ и ξ мы будем считать равными в семантическом смысле, если их значения равны независимо от фиксации (т.е. при любой фиксации) входных массивов, реализующих путь α . Очевидно, из синтаксического равенства переменных следует их семантическое равенство (однако обратное, как показывает предыдущий пример, имеет место не всегда). При определении степени инцидентности, фигурирующей в условиях теоремы, мы фактически использовали семантическое равенство переменных. Однако можно было бы использовать вместо семантического равенства также синтаксическое равенство. В таком случае мы получили бы несколько более сильную формулировку теоремы 2. Мы фактически докажем именно эту более сильную формулировку.

Заметим еще, что в графе GN концы прерывистых стрелочек можно передвигать по равным вершинам и от этого решения соответствующих систем неравенств не изменятся.

Теперь определим вычеркивание по правилу транзитивности произвольной вершины ζ из графа GN :

а) Рассматриваем все вершины ξ, η такие, что из ξ ведет дуга в ζ и из ζ в η (пусть p_1 и p_2 - соответственно веса этих дуг), и проводим из ξ в η новую дугу с весом p_1+p_2 .

б) Если в вершину ζ входят прерывистые стрелочки, то ищем вершину μ такую, что $\mu=\zeta$ согласно приведенному выше (синтаксическому) определению равенства, и концы этих стрелочек переносим на вершину μ ; если такая вершина μ не существует, то концы указанных стрелочек оставляем свободными.

в) Далее вычеркиваем вершину ζ вместе с дугами, входящими и выходящими из нее. Только перед этим проверяем, не появилась ли в результате шагов а и б петля (ζ,ζ) с весом больше 0 (что означает явное противоречие). В последнем случае выбираем какую-нибудь из оставшихся вершин ξ и проводим дугу (ξ,ξ) с весом больше 0 (чтобы в оставшемся графе также сохранялось явное противоречие).

г) Если в результате предыдущих шагов (точнее шага б) появилась какая-нибудь вершина ζ' с прерывистой стрелочкой, имеющей свободный конец, то с вершиной ζ' делаем в точности то же самое, что с вершиной ζ , т.е. опять выполняем шаги а,б,в, только вместо ζ берем ζ'. В результате вычеркивания ζ' опять могут появиться вершины ζ'' со свободными прерывистыми стрелочками, для них опять делаем то же самое, что и выше, и т.д.

В конечном итоге, наряду с вершиной ζ будут вычеркнуты также и все вершины со свободными прерывистыми стрелочками. Об оставшемся графе $(GN)_\zeta$ будем говорить, что он получен из GN вычеркиванием вершины ζ по правилу транзитивности. Фактически при этом, как мы видели, происходит вычеркивание также и других вершин; содержательно это те вершины, которые обозначают записи массива $\varkappa$, доступ к которым "опирается" на ζ.

В графе $(GN)_\zeta$ и тем более, в графах $((GN)_\zeta \ldots)_\mu$ могут существовать дуги (ξ, η) с весом p, где p - произвольное натуральное число:

$$\underset{\xi}{\circ} \xrightarrow{\ p\ } \underset{\eta}{\circ}$$

Такие дуги мы будем интерпретировать как неравенство

$$\eta \leq \xi - p$$

Пользуясь такой интерпретацией (что в случае $p = 0$ или 1 в точности совпадает с первоначальной интерпретацией) мы каждому графу $((GN)_\zeta \ldots)_\mu$ можем сопоставить определенную систему неравенств и говорить о ее решении. В дальнейшем мы будем говорить также о решении самого графа, имея в виду под этим решение соответствующей системы неравенств.

Переменные вида $t_k, u_l, \ldots$, где $t, u, \ldots$ - внутренние ячейки, будем называть в н у т р е н н и м и переменными. Внутренние переменные и переменные вида X_j, мы будем называть о с н о в н ы м и переменными. В системе $N(\alpha)$, кроме основных переменных, еще могут встречаться двойные переменные $\varkappa_p$, p - основная переменная, и переменные вида $\varkappa_c$, c - константа. Основные переменные, являющиеся индексами двойных переменных, будем называть и н д е к с н ы м и переменными системы $N(\alpha)$. Далее, основные переменные с наибольшими индексами, встречающиеся в $N(\alpha)$, будем называть а к т и в н ы м и переменными. Например, если $a_0, a_1, t_1, u_0, u_1, u_2, X_1, X_2, X_3$ – все основные переменные, входящие в $N(\alpha)$, то активными будут a_1, t_1, u_2, X_3. Содержательно активные переменные системы $N(\alpha)$ обозначают содержимое внутренних ячеек и последнюю запись массива X после прохождения пути α. Понятие активных переменных мы будем распространять также и на другие системы неравенств N и графы GN, содержащие переменные такого же вида, как $N(\alpha)$.

Пусть дано некоторое сопоставление D', которое каждой паре систем неравенств N, M сопоставляет некоторую конечную совокупность $D'(N,M)$ систем неравенств

$$D'(N,M)=\left\{R_1,\ R_2,\ldots,\ R_n\right\},$$

где каждая система R_i имеет вид

$$R_i=\begin{cases} N \\ S_i \\ M \end{cases},$$

S_i – зависящая от i, N и M система неравенств, в которой участвуют только активные переменные системы N и произвольные константы.

Используя сопоставление D', определим теперь новое сопоставление D, которое каждой системе неравенств

$$N(\alpha)=\begin{cases} \mathfrak{M}_1 \\ \vdots \\ \mathfrak{M}_r \end{cases}, \qquad \mathfrak{M}_i \text{ – подсистема, соответствующая команде } K_i,$$

сопоставляет конечную совокупность $DN(\alpha)$ систем неравенств

$$DN(\alpha)=\left\{N_1(\alpha),\ N_2(\alpha),\ \ldots,\ N_m(\alpha)\right\}$$

следующим образом:

$$\mathcal{N}_2 \overset{df}{=} D'(\mathfrak{M}_1, \mathfrak{M}_2),$$
$$\mathcal{N}_3 \overset{df}{=} \bigcup_{N \in \mathcal{N}_2} D'(N, \mathfrak{M}_3),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mathcal{N}_r \overset{df}{=} \bigcup_{N \in \mathcal{N}_{r-1}} D'(N, \mathfrak{M}_r),$$

и

$$DN(\alpha) \overset{df}{=} \mathcal{N}_r.$$

Такое сопоставление D в дальнейшем будем называть р а з б и е н и е м . Разбиение будем называть к о р р е к т н ы м, если для любого α объединение совокупностей решений системы $N_1(\alpha), \ldots, N_m(\alpha)$ дает в точности совокупность решений первоначальной системы $N(\alpha)$

Пусть C_1 и C_2 - соответственно наименьшая и наибольшая константа, встречающиеся в рассматриваемой программе.

Определим одно специальное разбиение D_0 . Для этого достаточно определить сопоставление D_0' , которым оно задается.

Если система $\mathfrak{M}_i$ соответствует команде вида $\varkappa(\zeta) \Longrightarrow \ldots$, т.е. $\mathfrak{M}_i$ имеет вид

либо $\left\{ \varkappa_\zeta < \varphi \right.$, либо $\left\{ \begin{array}{l} \varkappa_\zeta > \varphi \\ \varkappa_\zeta = \xi \end{array} \right.$, ζ - переменная,

то для любой системы неравенств N с активным ζ

$$D_0'(N, \mathfrak{M}_i) = \left\{ R_1, \ldots, R_{C_2 - C_1 + 3} \right\}$$

где

$$R_1 = \left\{ \begin{array}{l} N \\ \zeta < C_1, \\ \mathfrak{M}_i \end{array} \right. \quad R_2 = \left\{ \begin{array}{l} N \\ \zeta = C_1, \\ \mathfrak{M}_i \end{array} \right. \quad R_3 = \left\{ \begin{array}{l} N \\ \zeta = C_1 + 1, \\ \mathfrak{M}_i \end{array} \right. \ldots, R_{C_2 - C_1 + 3} = \left\{ \begin{array}{l} N \\ \zeta > C_2. \\ \mathfrak{M}_i \end{array} \right.$$

В остальных случаях

$$D_0'(N, \mathfrak{M}_i) = \begin{cases} N \\ \mathfrak{M}_i \end{cases}.$$

Легко видеть, что D_0 является коррективным разбиением. Если κ - число индексных переменных, входящих в $N(\alpha)$, то $D\ N(\alpha)$ разбивает $N(\alpha)$ на $(C_2 - C_1 + 3)^\kappa$ систем неравенств. Все эти системы характеризуются тем, что в каждой из них любая индексная переменная либо равна константе, либо меньше наименьшей константы программы, либо больше наибольшей константы программы.

Отметим еще, что корректным является также и тождественное разбиение $D_{\equiv}$:

$$D_{\equiv}\ N(\alpha) = \left\{ N(\alpha) \right\}.$$

Пусть теперь D - произвольное разбиение,

$$DN(\alpha) = \left\{ N_1(\alpha),\ N_2(\alpha),\ \dots,\ N_m(\alpha) \right\},$$

$N_j(\alpha)$ имеет вид:

$$N_j(\alpha) = \begin{cases} \mathfrak{M}_1 \\ s_{j1} \\ \mathfrak{M}_2 \\ \vdots \\ s_{jr-1} \\ \mathfrak{M}_r \end{cases}.$$

Согласно определению, в $s_{j\kappa}$ участвуют только активные переменные

системы $\begin{cases} \mathfrak{M}_1 \\ s_{j1} \\ \vdots \\ s_{j\kappa-1} \\ \mathfrak{M}_\kappa \end{cases}$, или, что то же самое, системы $\begin{cases} \mathfrak{M}_1 \\ \vdots \\ \mathfrak{M}_\kappa \end{cases}$

Введем обозначения начальных кусков $N_j(\alpha)$:

$$N_{jk} = \begin{cases} \mathfrak{M}_1 \\ s_{j1} \\ \vdots \\ s_{jk-1} \\ \mathfrak{M}_k \end{cases}$$

Наряду с N_{jk} будем рассматривать также и граф GN_{jk} изображающий систему N_{jk} .

Сопоставим теперь каждой системе $N_j(\alpha)$ некоторый граф $s_j(\alpha)$, который мы будем называть состоянием системы $N_j(\alpha)$. Определение $s_j(\alpha)$ индуктивное.

Положим $s_{j1} = GN_{j1}$.

Пусть уже определено s_{jk-1} и пусть s_{jk-1} и N_{jk-1} имеют одни и те же активные переменные. Тогда для построения s_{jk} сначала дополним граф s_{jk-1} в соответствии с системой неравенств

$$\begin{cases} s_{jk-1} \\ \mathfrak{M}_k \end{cases}$$

в точности так же, как при построении графа GN_{jk} из графа GN_{jk-1} . Это всегда возможно, так как s_{jk-1} и $\mathfrak{M}_k$ используют только активные переменные из GN_{jk-1} , а s_{jk-1} , согласно индуктивному предположению, содержит эти переменные. Полученный граф обозначим через s'_{jk-1} . Если команда K_k такова, что она новые переменные не вводит, т.е. при построении s'_{jk-1} из s_{jk-1} нам не требуется добавлять новые вершины, то $s_{jk} = s'_{jk-1}$. Если же при построении s'_{jk-1} из s_{jk-1} нам приходится добавлять новые вершины - переменные, то в результате этого некоторые переменные ζ , которые были активными в s_{jk-1} , могут перестать быть активными в s'_{jk-1} (например, если в s_{jk-1} были активными x_s и u_ℓ , то после K_i равной $X \Rightarrow u_\ell$ переменные X_s и u_ℓ

перестанут быть активными; вместо них появятся новые активные переменные x_{s+1} и $u_{\ell+1}$). В таком случае по правилу транзитивности вычеркиваем из S'_{jk+1} все такие вершины ζ . Далее, веса дуг, получившихся при этом больше $C_2 - C_1$, заменяем на $C_2 - C_1 + 1$ (C_1 и C_2 - соответственно наименьшая и наибольшая константы программы). Граф, который в результате этого получим из S'_{jk-1} обозначим через S_{jk} .

Теперь положим

$$S_j(\alpha) = S_{jr}.$$

На рис. 6 изображено $S_j(\alpha)$ при условии, что $N_j(\alpha)$ равно $N(\alpha)$ из предыдущего примера (см.также рис.5).

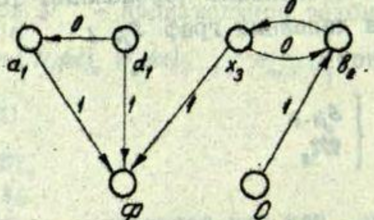


Рис. 6.

Определим теперь равенство двух состояний $S_j(\alpha)$ и $S_\ell(\beta)$: $S_j(\alpha) = S_\ell(\beta)$ если $S_j(\alpha)$ и $S_\ell(\beta)$ совпадают как графы с помеченными вершинами и дугами (прерывистые дуги тоже учитываются) при условии, что индексы у основных переменных стерты.

Из индукции построения состояния $S_j(\alpha)$ по $N_j(\alpha)$ непосредственно вытекает следующее свойство:

А. Пусть пути α и β заканчиваются на одной и той же вершине и пусть γ - произвольный путь, начинающийся с той вершины, на которой заканчиваются α и β . Пусть для некоторых $N_j(\alpha) \in DN(\alpha)$ и $N_\ell(\beta) \in DN(\beta)$

состояния

$$s_j(\alpha) = s_l(\beta).$$

Тогда для всех $N_v(\alpha+\gamma) \in DN(\alpha+\gamma)$ и $N_w(\beta+\gamma) \in DN(\beta+\gamma)$ вида

$$N_v(\alpha+\beta) = \begin{cases} N_j(\alpha) \\ \cdots \\ \cdots \\ \cdots \end{cases} \quad \text{и} \quad N_w(\beta+\gamma) = \begin{cases} N_l(\beta) \\ \cdots \\ \cdots \\ \cdots \end{cases}$$

соответствующие состояния

$$s_v(\alpha+\gamma) = s_w(\beta+\gamma).$$

Далее, под насыщенным графом $\tilde{G}$ для графа G будем понимать граф, который получается из G, если провести соответствующие дуги (если они еще не проведены) между всеми попарно равными (согласно приведенному выше определению) вершинами (т.е. если $\zeta = \xi$, то в $\tilde{G}$ должны быть дуги (ζ, ξ) и (ξ, ζ) с весом 0). Под весом ориентированного пути будем понимать сумму весов дуг, составляющих этот путь.

Будем говорить, что граф G удовлетворяет *условиям квазиреализуемости*, если в соответствующем насыщенном графе $\tilde{G}$:

1. Не имеется циклических путей с весом больше нуля.
2. Вес любого пути, ведущего из любой константной вершины c_2 в любую другую константную вершину c_1, не больше $c_2 - c_1$.

В случае, когда G не содержит двойных переменных, рассмотрение насыщенного графа $\tilde{G}$ для определения квазиреализуемости является лишним в том смысле, что условия 1 и 2 выполняются одновременно как в G, так и в $\tilde{G}$. Однако в случае, когда G содержит двойные переменные, как легко видеть, из выполнения условий 1 и 2 для $\tilde{G}$ еще не следует выполнения этих условий для G.

Далее будем говорить, что система неравенств N удовлетворяет условиям квазиреализуемости, если GN удовлетворяет условиям квазиреализуемости.

Согласно лемме 2 из [I] при отсутствии двойных переменных система неравенств $N(\alpha)$ имеет решение (следовательно, путь α реализуем) тогда и только тогда, когда $N(\alpha)$ удовлетворяет условиям квазиреализуемости. Однако, при наличии двойных переменных условия квазиреализуемости являются только необходимыми условиями реализуемости пути α : если $N(\alpha)$ имеет решение, то оно обязательно обладает условиями квазиреализуемости.

Рассмотрим теперь вычеркивание по правилу транзитивности произвольной вершины ζ из графа G (в результате мы получим граф $(G)_\zeta$). Легко убедится, что G и $(G)_\zeta$ одновременно будет удовлетворять или неудовлетворять условиям квазиреализуемости. Отсюда и из определения состояния $S_j(\alpha)$ получаем следующее важное свойство:

Б. $N_j(\alpha)$ и $S_j(\alpha)$ одновременно удовлетворяют или неудовлетворяют условиям квазиреализуемости.

Итак, пусть произвольным образом фиксировано корректное разбиение D ,

$$DN(\alpha) = \left\{N_1(\alpha), \ldots, N_m(\alpha)\right\},$$

$S_j(\alpha)$ - состояние, соответствующее $N_j(\alpha)$. Определим теперь новое состояние $S(\alpha)$:

$$S(\alpha) = \left\{S_1(\alpha), \ldots, S_m(\alpha)\right\}.$$

Там, где могут возникнуть недоразумения, состояния $S_j(\alpha)$ будем называть частными состояниями, а состояние $S(\alpha)$ - полным состоянием.

Два полных состояния $S(\alpha)$ и $S(\beta)$ будем называть равными $(S(\alpha) = S(\beta))$, если для всякого частного состояния $S_j(\alpha) \in S(\alpha)$ существует частное состояние $S_\ell(\beta) \in S(\beta)$ такое, что $S_j(\alpha) = S_\ell(\beta)$, и обратно.

Далее, будем говорить, что путь α квазиреализуем, если условиям квазиреализуемости удовлетворяет хотя бы одна из систем неравенств $N_1(\alpha), \dots, N_m(\alpha)$. Согласно свойству Б это равносильно тому, что условиям квазиреализуемости удовлетворяет хотя бы одно из частных состояний $S_1(\alpha), \dots, S_m(\alpha)$. В последнем случае мы будем говорить, что полное состояние $S(\alpha)$ удовлетворяет условиям квазиреализуемости. Отсюда и из свойства А вытекает следующий аналог леммы 3 из [I] :

ЛЕММА 2. Если пути α и β программы T, оканчивающиеся на одной и той же команде q, квазиреализуемы и $S(\alpha)=S(\beta)$, то для любого пути γ, начинающегося с q, из квазиреализуемости пути $\alpha+\gamma$ следует квазиреализуемость пути $\beta+\gamma$.

Если мы будем рассматривать произвольную программу T и всевозможные пути α в этой программе, то может оказаться, что число различных состояний $S(\alpha)$ будет бесконечное. Это может возникнуть за счет того, что в частных состояниях $S_j(\alpha)$, кроме активных переменных (их число ограничено), сохраняются и те двойные переменные, которые на них "опираются", а их число для различных α может быть неограничено, если глубина инцидентности программы неограничена. Однако если глубина инцидентности ограничена некоторым число s, то число двойных переменных, "опирающихся" на одно переменное, не превышает s. Отсюда следует, что если T удовлетворяет условиям теоремы, т.е. имеет ограниченную степень инцидентности, то число различных частных и, следовательно, число различных полных состояний программы T ограничено. Именно для этой цели были введены ограничения на программы в условиях теоремы.

Определим теперь дерево реализуемости программы в точности так же, как в [I] , имея в виду под состоянием $S(\alpha)$ полное состояние пути α определенное выше, а под реализуемостью пути α - квазиреализуемость пути α (при разбиении D). Так как согласно изложенному выше число различных состояний $S(\alpha)$ конечное, то приведенный в [I] алгоритм построения дерева реализации применим и в нашем случае. Получающееся дерево реализуемости в нашем случае зависит, вообще говоря, от фиксации разбиения D .

Из построения дерева реализуемости и леммы 2 непосредственно вытекает

ЛЕММА 3. Любая ветвь дерева реализуемости как путь программы квазиреализуема.

Если путь программы, задаваемый некоторой ветвью h дерева реализуемости, содержит ветвь δ программы, то будем говорить, что ветвь h дерева реализуемости содержит ветвь δ программы.

ЛЕММА 4. Ветвь δ программы квазиреализуема тогда и только тогда, когда существует СТОП-ветвь дерева реализуемости, которая содержит ветвть δ .

Достаточность условий леммы 4 вытекает из леммы 3. Необходимость условий леммы 4 доказывается в точности так же, как необходимость условий леммы 5 из [I] , только вместо леммы 3 из [I] надо использовать приведенную выше аналогичную лемму 2.

Далее, из корректности разбиения D и необходимости условий квазиреализуемости для существования решения у системы $N_j(\alpha)$ вытекает

ЛЕММА 5. Если ветвь δ программы T реализуема (т.е. принадлежит реализуемому пути), то она также и квазиреализуема (т.е. принадлежит квазиреализуемому пути).

Из лемм 4 и 5 свою очередь вытекает следующая важная

ЛЕММА 6. Пусть при заданном корректном разбиении D система примеров Σ такова, что она реализует все СТОП-ветви дерева реализуемости программы T. Тогда система Σ является полной системой примеров для программы T.

Пусть N - система неравенств, в которой, вообще говоря, встречаются также и двойные переменные. Рассмотрим соответствующую насыщенную систему $\tilde{N}$, которая получается из N добавлением всевозможных равенств $\zeta = \xi$, которые получаются согласно приведенному выше (синтаксическому) определению равенства (переменные ζ и ξ, которые согласно этому понятию равенства не являются равными, будем называть различными). Ясно, что совокупности решений систем N и $\tilde{N}$ совпадают. Рассмотрим теперь все двойные переменные, входящие в $\tilde{N}$, как обычные переменные, не зависящие от значения индекса. В результате такой интерпретации $\tilde{N}$ превратится в традиционную систему неравенств. Систему $\tilde{N}$ при указанной интерпретации будем называть традиционной системой неравенств, соответствующей системе N.

ЛЕММА 7. Если некоторое решение соответствующей традиционной системы неравенств $\tilde{N}$ таково, что все различные индексные переменные принимают разные значения, то это решение является также и решением для исходной системы N.

Справедливость данной леммы вытекает из того, что если у двойных переменных разные значения индексов, то между ними не существует никаких других соотношений (равенств или неравенств), кроме тех, которые указаны в $\tilde{N}$, так как единственный случай, когда между двойными переменными, и, следовательно, между другими переменными могут появляться новые соотношения - это когда оказываются равными их индексы; в этом случае должны быть равными также и сами двойные переменные.

Рассмотрим переменные системы N , которые ограничены некоторой константой не более чем с одной стороны (ζ ограничено сверху (снизу) константой c , если в $G\tilde{N}$ существует путь, ведущий из c в ζ (из ξ в c). Такие переменные мы будем называть с в о б о д н ы м и.

ЛЕММА 8. Существует алгоритм A , который для любой традиционной системы неравенств $\tilde{N}$, удовлетворяющей условиям квазиреализуемости, строит решение такое, что все различные свободные переменные принимают разные значения.

Алгоритм A аналогичен алгоритму, описанному в [I] при доказательстве леммы 2. Единственная разница состоит в том, что дополнительно надо требовать, чтобы значения свободным переменным присваивались в конце процесса и чтобы значение каждого следующего свободного переменного выбиралось отличным от значений предыдущих переменных (а это всегда возможно).

Рассмотрим теперь разбиение D_0 . Пусть

$$D_0 N(\alpha) = \left\{ N_1^0(\alpha), \ldots, N_m^0(\alpha) \right\}.$$

Из определения D_0 следует, что каждая система $N_j^0(\alpha)$, удовлетворяющая условиям квазиреализуемости (т.е. не содержащая явные противоречия вида $\zeta < c' \,\&\, \zeta > c''$,где $c' < c''$), должна обладать тем свойством, что любая входящая в нее индексная переменная либо равна константе, либо свободна.

ЛЕММА 9. При разбиении D_0 любой квазиреализуемый путь является также реализуемым и существует алгоритм B, который для каждого квазиреализуемого пути α строит пример, реализующий этот путь.

Для доказательства леммы рассмотрим произвольный квазиреализуемый путь α. Это означает, что для некоторого j $N_j^0(\alpha)$ удовлетворяет условиям квазиреализуемости. Рассмотрим соответствующую традиционную систему неравенств $\tilde{N}_j^0(\alpha)$. Она тоже удовлетворяет условиям квазиреализуемости. Согласно лемме 8 существует алгоритм A, который строит решение традиционной системы $\tilde{N}_j^0(\alpha)$, при котором все различные свободные переменные принимают разные значения, в том числе и свободные индексные переменные. Но у системы $N_j^0(\alpha)$ любая входящая в нее индексная переменная либо равна константе, либо свободна. Отсюда по лемме 7 получаем, что решение соответствующей традиционной системы, построенной с помощью алгоритма A, является также и решением системы $N_j^0(\alpha)$. Таким образом искомый алгоритм B сводится к тому, что по α он строит $D_0 N(\alpha) = \{N_1^0(\alpha), \ldots, N_m^0(\alpha)\}$ и для каждого $N_j^0(\alpha)$ проверяет, не выполняются ли для него условия квазиреализуемости. Из квазиреализуемости α следует, что для некоторого $N_j^0(\alpha)$ эти условия выполняются. Рассматриваем соответствующую традиционную систему $\tilde{N}_j^0(\alpha)$ и к ней применяем алгоритм A из леммы 8. Получаем решение системы $N_j^0(\alpha)$. Согласно лемме I оно дает пример, реализующий путь α.

Для завершения доказательства теоремы разюмируем получившийся алгоритм построения полной системы примеров для программ T, удовлетворяющих условиям теоремы:

По программе T строим дерево реализуемости при разбиении D_0. Согласно лемме 3 любая ветвь дерева реализуемости как путь программы квазиреализуема. Рассматриваем все СТОП-ветви дерева реализуемости и применяем к ним алгоритм B из леммы 9. Согласно лемме 6 полученная система примеров является полной.

Теорема доказана.

ЗАМЕЧАНИЕ I. Опишем один метод, который во многих случаях позволяет принципиально упростить построение полных систем примеров для программ, удовлетворяющих условиям теоремы. Вместо разбиения D_0 возьмем тождественное разбиение $D_=$. В этом случае фактически никакого разбиения системы не будет и $S(\alpha)$ будет то состояние , которое непосредственно получается по $N(\alpha)$ (как при определении частного состояния). Строим, как и выше, дерево реализуемости, только относительно нового состояния $S(\alpha)$. Затем , рассматривая все СТОП-ветви построенного дерева реализуемости, составляем для них системы $N(\alpha)$. Далее, рассматриваем соответствующие традиционные системы $\tilde{N}(\alpha)$ и для каждой из них строим решение согласно какому-нибудь заранее фиксированному алгоритму решения традиционных систем неравенств (для дальнейшего важно, чтобы этот алгоритм различным индексным переменным выбирал по возможности разные значения). Предположим теперь, что эти решения оказались такими, что им удовлетворяют также и исходные системы $N(\alpha)$, в которых участвуют двойные переменные. В таком случае система примеров, соответствующая этим решениям, будет реализовать все СТОП-ветви построенного дерева реализуемости и, согласно лемме 6, будет являться полной системой примеров для данной программы.

В общем случае лемма 6 позволяет использовать также и другие разбиения, промежуточные между $D_=$ и D_0 . В этом смысле разбиение D_0 можно рассматривать как предельное разбиение, при котором описанный процесс построения полной системы примеров обязательно оборвется.

Рассмотрим построение полной системы примеров для программы, изображенной на рис. 2. В качестве разбиения возьмем $D_{\text{ш}}$. На рис. 7 изображен фрагмент дерева реализуемости, СТОП-ветви которого уже содержат полную систему примеров. Полученная полная система примеров (вместе с некоторой дополнительной информацией) изображена в

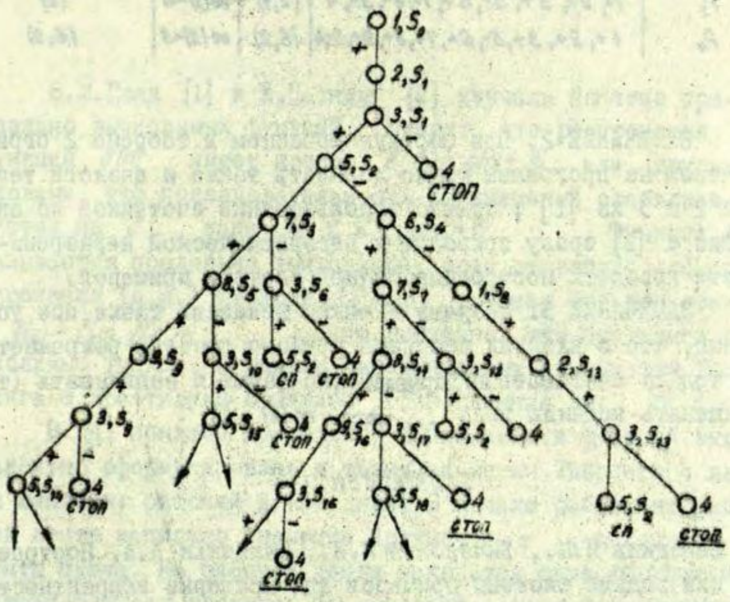


Рис. 7.

таблице I. Как уже было сказано, рассматриваемая программа написана ошибочно: в выходном массиве она пропускает некоторые нули. Легко убедиться, что построенная система примеров обнаруживает эту ошибку.

Таблица I

Обозначения	Пути	Примеры		Результат
		x	æ	y
P_1	1+, 2+, 3+, 5+, 7-, 3-, 4	(5,-1)	æ(-1)+φ	(5)
P_2	1+, 2+, 3+, 5-, 6-, 1+, 3-, 4	(4,0,2)	–	(4,2)
P_3	1+, 2+, 3+, 5-, 6+, 7+, 8-, 3-, 4	(2,1)	æ(1)-4	(2)
P_4	1+, 2+, 3+, 5-, 6+, 7+, 8+, 9+, 3-, 4	(6,2)	æ(2)-3	(6,2)

ЗАМЕЧАНИЕ 2. При сформулированном в теореме 2 ограничении на программы можно доказать также и аналоги теорем 2 и 3 из [I] ; однако использование счетчиков по аналогии с [2] сразу приводит к алгоритмической неразрешимости проблемы построения полной системы примеров.

ЗАМЕЧАНИЕ 3. Теорему 2 можно доказать также при условии, что с входных массивов прямого доступа разрешается не только считывать информацию, но также и записывать (т.е. применять команды вида ... $\Longrightarrow$ æ(t)).

ЛИТЕРАТУРА

I. Барздинь Я.М., Бичевский Я.Я., Калниньш А.А. Построение полной системы примеров для проверки корректности программ.-"Учен.зап.Латв. ун-та", 1974.т.210.

2. Калниньш А.А., Бичевский Я.Я., Барздинь Я.М. Разрешимые и неразрешимые случаи проблемы построения полной системы примеров.-"Уч. зап. Латв. ун-та",1974.т.210.

О СЛОЖНОСТИ И ОПТИМАЛЬНОСТИ ПРЕДЕЛЬНЫХ ВЫЧИСЛЕНИЙ

Р.В.Фрейвалд

Э.М.Голд [1] и Х.Патнам [2] изучали понятие предельно вычислимых функций. Говорят, что рекурсивная функция $g(n)$ имеет предел $b\ (\lim\limits_n g(n)=b)$ или, другими словами, что последовательность ее значений стабилизируется на b, если $\exists n_0 \forall_n \geq n_0 (g(n)=b)$. Функция $f(x)$ называется предельно вычислимой, если существует общерекурсивная (о.р.) функция $\tilde{f}(x,n)$, такая что для всех x $f(x)=\lim\limits_n f(x,n)$. Было доказано, что предельно вычислимые функции и только они вычислимы на машинах Тьюринга с креативным оракулом (определение см. [3]).

В [4] понятие предельной вычислимости функций эквивалентно сформулировано в терминах машин Тьюринга с двумя лентами: рабочей и выходной. В начале работы на рабочей ленте записано значение аргумента x, выходная лента пуста. На рабочей ленте находится одна обычная читающая-пишущая головка, на выходной - одна только-пишущая головка, которая может стоять на месте или двигаться вправо, но не может двигаться влево. Во время работы машины эта головка печатает последовательность натуральных чисел $k_1, k_2, k_3, \dots$ с разделительными знаками между их записями. Будем считать запись очередного числа законченной, если за этой записью напечатан хотя бы один разделительный знак и головка уже ушла вправо от этого разделительного знака. Между двумя соседними числами допускается произвольное число разделительных знаков. Таким образом, любое заполнение машиной выходной ленты или ее части определяет пустую, конечную или бесконечную последовательность тех натуральных чисел, печать которых закончена. Пределом выходной последовательности будем называть последнее полностью напечатанное число (если последовательность конечная) и число θ , если все напечатанные числа, кроме конечного числа первых, равны θ (если последовательность бесконечная). В остальных случаях предел выходной последовательности не определен. Функцией, которую предельно вычисляет машина $\mathfrak{M}$, будем называть функцию, сопоставляющую каждому значению аргумента x предел выходной последовательности $K_1, K_2, K_3, \ldots$ напечатанной машиной $\mathfrak{M}$ при работе на x .

Такое определение сразу приводит к мысли о сложностях предельных вычислений.

При обычном (непредельном) вычислении функции процесс вычисления при получении результата останавливается, что дает возможность окончательно подсчитать затраченное время, емкость и другие характеристики. В случае предельных вычислений время бесконечно, емкость, режим, число колебаний и другие подобные характеристики, как правило, тоже.

Однако имеются достаточно естественные характеристики процесса предельного вычисления, которые принимают конечное значение, если предельно вычислимая функция определена, например:

а) <u>сигнализирующая времени</u> (для каждого x сигнализирующая $t(x)$ равна числу тактов работы машины, пока на выходной ленте будет закончено печатание такого K_n , что все последующие выходные значения, которые будут полностью напечатаны, равны K_n ; если такое K_n не существует, то $t(x) = \infty$) ,

б) <u>сигнализирующая емкости</u> (для каждого x сигнализирующая $s(x)$ равна числу ячеек рабочей ленты, использованных машиной до такта $t(x)$; если $t(x) = \infty$, то по определению $s(x) = \infty$).

По образцу а) и б) можно ввести аналоги и другим естественным сигнализирующим обычных вычислений. Впрочем, для предельных вычислений можно рассматривать и специфические сигнализирующие, не имеющие аналогов для обычных вычислений, например

в) сигнализирующая числа изменений гипотезы (для каждого x сигнализирующая $H(x)$ равна числу таких n, что в выходной последовательности $K_n \neq K_{n-1}$; если выходная последовательность пуста, то $H(x)$ не определена).

Большую часть теории сложностей обычных вычислений можно построить на основе двух аксиом М.Блюма [5,6]. Фиксируется некоторая главная вычислимая нумерация $\{\varphi_i\}$ всех одноместных частично рекурсивных (ч.р.) функций (например, естественная тьюрингова - через коды программ машин Тьюринга). Каждому i (т.е. по существу, каждой машине) сопоставляется функция Φ_i со свойствами:

1) функция $\lambda i \lambda x\, \Phi_i(x)$ имеет ту же область определения, что и $\lambda i \lambda x\, \varphi_i(x)$,

2) функция $\lambda i \lambda x\, \Phi_i(x)$ имеет рекурсивный график.

Пусть $\psi_i(x)$ - это функция, предельно вычисляемая машиной $\mathfrak{M}_i$. Какие похожие свойства нужно требовать при сопоставлении каждому i сигнализирующей функции $\Psi(x)$?

Дж.Ходжаев [7] показал, что основные факты аксиоматической теории сложностей остаются в силе, если в аксиомах и теоремах везде рассматривать функции, вычислимые на машинах с фиксированным оракулом. Предельная вычислимость функций равносильна вычислимости с креативным оракулом. Поэтому в качестве аналогов аксиом Блюма естественно рассматривать:

1) функция $\lambda i \lambda x\, \Psi_i(x)$ имеет ту же область определенности, что и $\lambda i \lambda x\, \psi_i(x)$,

2) функция $\lambda i \lambda x\, \Psi_i(x)$ имеет предельно рекурсивный график.

Отметим, что для сигнализирующих времени и емкости (но не для сигнализирующей числа изменений гипотез) свойство 2 можно усилить:

2 а) трехместный предикат "$\Psi_i(x) \geq a$ или $\Psi_i(x)$ не определена" рекурсивно перечислим.

Впрочем, это не удивительно - для временной, емкостной и других "естественных" сигнализирующих обычных вычислений тоже можно усилить вторую аксиому Блюма: рассматриваемый трехместный предикат примитивно рекурсивен.

Для краткости изложения дальнейших рассуждений введем следующие соглашения. Всюду определенные предельно вычислимые функции будем называть предельно общерекурсивными (п.о.р.) функциями. Функции, принимающие только значения 0 и 1, условно будем называть предикатами. Если некоторое свойство выполняется для всех натуральных чисел x, кроме конечного числа, то будем говорить, что это свойство выполняется для почти всех x.

Из результатов Дж.Ходжаева вытекают следующие предложения 1, 2 и (в несущественно более слабой форме) предложение 3.

ПРЕДЛОЖЕНИЕ 1. (Аналог теоремы М.Рабина [8,6]). Для любого сигнализирующего оператора со свойствами 1 и 2 и для любой п.о.р. функции $h(x)$ существует такой п.о.р. предикат $f(x)$, что для всех i, если $\varphi_i = f$, то для почти всех x $\Psi_i(x) \geq h(x)$.

ПРЕДЛОЖЕНИЕ 2. (Аналог теоремы М.Блюма [5]). Для любого сигнализирующего оператора со свойствами 1 и 2 и для любой двуместной п.о.р. функции r существует п.о.р. предикат $f(x)$, такой, что для любого предельного вычисления φ_i предиката f существует другое его предельное вычисление φ_j, при котором для почти всех x $\Psi_i(x) > r(x, \Psi_j(x))$.

ПРЕДЛОЖЕНИЕ 3. (Аналог теоремы о проблемах*)). Для

*) Для обычных вычислений теорема о проблемах была доказана Б.А.Трахтенбротом [6] и независимо, но позже А.Бородиным [9].

любого сигнализирующего оператора со свойством 2 и для любых п.о.р. функций $a(x)$ и $r(x,y)$, если для всех x,y имеет место $r(x,y) \geqslant y$, то существует такая п.о.р. функция $b(x)$, что для всех x $b(x) \geqslant a(x)$ и для всех $x > j$ из $\Psi_j(x) \geqslant b(x)$ следует $\Psi_j(x) > r(x, b(x))$.

ДОКАЗАТЕЛЬСТВО фактически копирует доказательство теоремы о пробелах, данное П.Янгом [10]. Из свойства 2 вытекает существование такой о.р. функции $c(j,x,n)$, что $\lim\limits_n c(j,x,n) = \Psi_j(x)$, если $\Psi_j(x)$ определена и $\lim\limits_n c(j,x,n) = +\infty$, если $\Psi_j(x)$ не определена. Пусть $\tilde{a}(x,n)$ и $\tilde{r}(x,y,n)$ - такие о.р. функции, что $a(x) = \lim\limits_n \tilde{a}(x,n)$ и $r(x,y) = \lim\limits_n \tilde{r}(x,y,n)$. Для построения $\tilde{b}(x)$ положим $d_{x+1,n} = \tilde{a}(x,n)$ и для $0 < i \leqslant x+1$

$d_{i-1,n} = \tilde{r}(x, d_{i,n}, n) + 1$. Таким образом, для больших n $d_{x+1,n} < d_{x,n} < d_{x-1,n} < \dots < d_{0,n}$. Промежутков $[d_{i,n}, d_{i-1,n})$ у нас всего $x+1$, значит, среди них должен найтись такой $[d_{i_0,n}, d_{i_0-1,n})$, который не содержит ни одного из значений

$c(0,x,n), c(1,x,n), \dots, c(x-1,x,n)$. Определяем тогда

$$\tilde{b}(x,n) = d_{i_0,n} \quad \text{и} \quad b(x) = \lim_n \tilde{b}(x,n) .$$

Для предельных вычислений (в отличие от обычных) все же не все естественные сигнализирующие удовлетворяют приведенным выше аксиомам. Например, в [11,12] при изучении некоторых задач индуктивного вывода оценивалась, по существу, следующая характеристика сложности.

<u>Сигнализирующая числа различных гипотез</u> (для каждого x сигнализирующая $Y(x)$ равна числу попарно различных чисел, встречающихся в последовательности $k_1, k_2, \dots$ напечатанной при работе машины на значении аргумента x).

Эта сигнализирующая не удовлетворяет свойству 1. Можно, конечно, добавить к определению сигнализирующей оговорку "если предел последовательности $k_1, k_2, \dots$

не существует, то $\mathcal{Y}(x)$ не определена", но тогда будет нарушено свойство 2.

Предложение 3, впрочем, имеет место для этой сигнализирующей, так как в нем не требуется выполнения свойства 1. Другие результаты аксиоматической теории сложностей выполняются лишь в несколько ослабленной форме. Например, легко доказать следующий аналог предложения 1.

ПРЕДЛОЖЕНИЕ 4. Для любой п.о.р. функции $h(x)$ существует такая п.о.р. функция $f(x)$, что для всех i, если $\psi_i = f$, то для почти всех x $\mathcal{Y}_i(x) \geqslant h(x)$.

Усилить предложение 4 требованием, чтобы $f(x)$ принимала только значение 0 и 1, невозможно, так как любой п.о.р. предикат можно вычислить с сигнализирующей $\mathcal{Y}(x) \leqslant 2$.

Автор, к сожалению, не видит, как разумно сформулировать в виде аксиом те свойства сигнализирующей числа различных гипотез, которые обеспечивают справедливость предложения 4, не обеспечивая при этом указанного усиления. В первую очередь, конечно, было бы желательно видоизменить свойство 1:

1а) область определения функции $\lambda i \ \lambda x \ \psi_i(x)$ содержится целиком в области определения функции $\lambda i \ \lambda x \ \Psi_i(x)$

Однако этого недостаточно, так как "сигнализирующая" $\Psi(x) = 0$ удовлетворяет свойствам 1а и 2, но для нее предложение 4 не имеет места.

Аксиоматическая теория сложностей не исчерпывает все содержательно интересные результаты теории сложностей обычных вычислений. Например, она не охватывает все положительные результаты о существовании оптимальных (в различных смыслах) вычислений.

Уточним понятие оптимальности сигнализирующей функции.

ОПРЕДЕЛЕНИЕ 1. Пусть $\{g_i(y)\}$ - семейство всюду определенных одноместных функций. Функцию $h(x)$ назовем сильно (слабо) оптимальной с точностью до семейства $\{g_i(y)\}$ для вычисления $f(x)$, если:

1) существует машина, вычисляющая $f(x)$ с сигнализирующей, не превосходящей $h(x)$,
2) для любой машины, вычисляющей $f(x)$, существует такое i , что для почти всех x (соответственно: для бесконечно многих x) сигнализирующая не меньше $g_i(h(x))$.

Легко видеть, что свойство оптимальности не меняется при добавлении или изъятии из семейства $\{g_i(y)\}$ таких функций, которые для почти всех y больше y . При любых $h(x)$ и $f(x)$ функция $h(x)$ является оптимальной для $f(x)$ с точностью до такого семейства, которое содержит функцию $g_i(y)$, для почти всех y равную 0.

Наибольший интерес представляет понятие оптимальности с точностью до семейств, все функции $g_i(y)$ которых а) не превышают y , б) растут по возможности быстро.

Ниже будут специально рассмотрены оптимальности с точностью до трех семейств $\{g_i(y)\}$:
1) семейство, все функции которого равны тождественной функции: $g_i(y) = y$ - в этом случае мы будем говорить об абсолютной оптимальности;
2) семейство $g_i(y) = y - i$ - в этом случае мы будем говорить об аддитивной оптимальности;
3) семейство $g_i(y) = \left[\frac{y}{i+1}\right]$ - в этом случае мы будем говорить о мультипликативной оптимальности.

Не используя новых идей по сравнению с известными доказательствами аналогичных теорем для непредельных вычислений, может быть доказано

ПРЕДЛОЖЕНИЕ 5. Пусть машина $\mathfrak{M}$ предельно вычисляет предикат $f(x)$, причем сигнализирующая времени у этой машины равна $t_{\mathfrak{M}}(x)$, а сигнализирующая емкости - $S_{\mathfrak{M}}(x)$. Для произвольной константы $c > 0$ существует другая машина $\mathfrak{M}'$, вычисляющая этот же предикат с сигнализирующими емкости и времени:

$$S_{\mathfrak{M}'}(x) \leqslant \max\left\{|x|+1, \frac{S_{\mathfrak{M}}(x)}{c}\right\}$$

$$t_{\mathfrak{m}'}(x) \leqslant |x|^2 + \frac{t_{\mathfrak{m}}(x)}{c},$$

где $|x|$ - длина записи значения аргумента x.

Это предложение показывает, что быстро растущие функции не могут быть сильно и даже слабо аддитивно оптимальными сигнализирующими емкости или времени.

ПРЕДЛОЖЕНИЕ 6. Для любой всюду определенной сигнализирующей емкости $h(x)$ существует такой п.о.р. предикат $f(x)$, что $h(x)$ является слабо мультипликативно оптимальной сигнализирующей емкости для вычисления $f(x)$.

ДОКАЗАТЕЛЬСТВО. Существуют универсальные машины предельного вычисления. Моделируя работу машины $\mathfrak{M}$ на слове P, универсальная машина обрабатывает пару $\{$шифр $\mathfrak{M}$, код слова $P\}$ и выдает в точности ту же последовательность выходных символов. Обозначим через $s_{\mathfrak{M}}(P)$ сигнализирующую емкости машины $\mathfrak{M}$ и через $\hat{s}_{\mathfrak{M}}(P)$ - длину участка ленты, который затрачивает универсальная машина до выдачи первого стабилизированного выхода значения (включительно). Тогда $\hat{s}_{\mathfrak{M}}(P)$ назовем приведенной сигнализирующей емкости машины $\mathfrak{M}$ относительно данной универсальной машины.

Очевидно, можно построить настолько экономную универсальную машину, чтобы для любой машины $\mathfrak{M}$ существовала константа $c_{\mathfrak{M}}$, зависящая от $\mathfrak{M}$, но не зависящая от P, такая что всех $\mathfrak{M}$ и P $\hat{s}_{\mathfrak{M}}(P) \leqslant c_{\mathfrak{M}} s_{\mathfrak{M}}(P)$. Зафиксируем для дальнейшего доказательства именно такую универсальную машину.

Обозначим через $\ell(x)$ одну из канторовских одноместных функций, обладающих свойством каждое натуральное число принимать в качестве значения бесконечно много раз. Пусть $\mathfrak{M}_i$ - i-ая машина Тьюринга в нумерации, сопряженной с зафиксированной универсальной машиной, а $\hat{S}_i(x)$ - приведенная сигнализирующая емкости машины $\mathfrak{M}_i$.

Определим предикат $f(x)$ как функцию, предельно вычисляемую следующей машиной $\mathfrak{M}'$ с двухэтажной рабочей лентой, один этаж которой используется для вычисления $h(x)$, а другой - для проверки "$\hat{S}_{\ell(x)}(x) > h(x)$?" Определенные трудности в построении такой машины связаны с тем, что $h(x)$ вычислима лишь предельно.

В первый такт машина $\mathfrak{M}'$ выдает выходное значение 1. Далее, выдача нового выходного значени происходит в каждый такт работы машины $\mathfrak{M}'$. В большинстве случаев (если только в описании работы $\mathfrak{M}'$ не оговорено иное) на выходе механически повторяется значение, выданное на предыдущем такте.

Для вычисления значения функции $h(x)$ используется то, что $h(x)$ - сигнализирующая емкости некоторой машины $\mathfrak{M}''$. На первом этаже рабочей ленты машины $\mathfrak{M}'$ моделируется внутренняя работа $\mathfrak{M}''$, но выходные значения $\mathfrak{M}''$ не печатаются. Первой гипотезой h_1 о значении $h(x)$ является число ячеек, использованное машиной $\mathfrak{M}''$ до такого момента, когда $\mathfrak{M}''$ выдает первое выходное значение.

Легко видеть, что это моделирование и вычисление значения h_1 можно провести на отрезке рабочей ленты длины h_1. Когда h_1 вычислено, моделирование работы $\mathfrak{M}''$ временно приостанавливается (чтобы $\mathfrak{M}'$ не тратила лишний объем памяти) и на втором этаже рабочей ленты $\mathfrak{M}'$ моделируется внутренняя работа (без выдачи выходных значений) машины $\mathfrak{M}_{\ell(x)}$ на аргументе x. Это моделирование проводится либо до момента, когда $\mathfrak{M}_{\ell(x)}$ на x собирается использовать длину ленты, превышающую h_1 (точнее: когда приведенная емкость превышает h_1), либо до момента, когда обнаруживается, что $\mathfrak{M}_{\ell(x)}$ на x зациклилась на отрезке ленты, приведенная длина которого не превышает h_1. В результате определяется значение $\delta(x,1)$, равное 0 или 1 и отличающееся от последнего выходного значения, полностью напечатанного машиной $\mathfrak{M}_{\ell(x)}$

на x° за обозреваемое время.

После этого машина $\mathfrak{M}'$ вместо предыдущего выходного значения начинает на каждом такте выдавать $b(x,1)$.

Далее, на первом этаже рабочей ленты $\mathfrak{M}'$ снова продолжается моделирование внутренней работы $\mathfrak{M}''$. Это продолжается до тех пор, пока $\mathfrak{M}''$ не изменит выходное значение. Если это случится, то отмечается число h_2 ячеек, использованных машиной $\mathfrak{M}''$ до этого момента $(h_2 \geq h_1)$. Если $h_2 = h_1$, то $b(x,2) = b(x,1)$. Если $h_2 > h_1$, то для определения $b(x,2)$ проводится моделирование работы $\mathfrak{M}_{e(x)}$ на x описанным выше способом (только вместо значения h_1 используется значение h_2).

После этого машина $\mathfrak{M}'$ вместо предыдущего выходного значения начинает на каждом такте выдавать $b(x,2)$ и т.д.

Проверка требуемых свойств предиката $f(x)$, предельно вычисляемого машиной $\mathfrak{M}'$, не представляет труда.

Предложение доказано.

Автору не удалось выяснить, можно ли предложение 6 усилить, потребовав с и л ь н у ю мультипликативную оптимальность сигнализирующей $h(x)$. Неизвестно также, справедлив ли аналог предложения 6 для сигнализирующей времени.

Перейдем теперь к изучению оптимальности в смысле сигнализирующей числа изменений гипотезы (сокращенно: сигнализирующей ч.и.г.).

ПРЕДЛОЖЕНИЕ 7. Всюду определенная функция $h(x)$ является сигнализирующей ч.и.г. некоторой машины тогда и только тогда, когда $h(x)$ можно представить как предел $\lim_n \tilde{h}(x,n)$ такой общерекурсивной функции $\tilde{h}$, которая при каждом значении первого аргумента является неубывающей по второму аргументу.

ДОКАЗАТЕЛЬСТВО очевидно.

ПРЕДЛОЖЕНИЕ 8. Для любой всюду определенной сигнализирующей ч.и.г. h существует такой п.о.р. предикат f что h является слабо абсолютно оптимальной сигнализирующей ч.и.г. для вычисления f .

ДОКАЗАТЕЛЬСТВО. Пусть $\tilde{h}(x,n)$ - функция из предложения 7, соответствующая функции h . Обозначим n-ое выходное значение $(n>0)$ машины $\mathfrak{M}$, работающей на x , через $\tilde{f}(x,n)$. Если $\mathfrak{M}_{\ell(x)}$ на x в течение n тактов не заканчивает печатание ни одного выходного значения, то $\tilde{f}(x,n)=0$. Если $\mathfrak{M}_{\ell(x)}$ на x в течение n тактов меняет выходное значение не менее $\tilde{h}(x,n)$ раз, то $\tilde{f}(x,n)=\tilde{f}(x,n-1)$. В остальных случаях выясняется последнее выходное значение, напечатанное $\mathfrak{M}_{\ell(x)}$ при работе на x за n тактов, и $\tilde{f}(x,n)=0$, если это значение отлично от нуля, и $\tilde{f}(x,n)=1$ в противном случае.

С предложением 8 контрастирует основной результат статьи.

ТЕОРЕМА 1. Для любой всюду определенной сигнализирующей ч.и.г. h_1 существует такая п.о.р. функция h_2 , что:

1) для всех x $h_1(x)<h_2(x)<(2+x)(1+h_1(x))$

2) существует такой п.о.р. предикат f , что h_2 является сильно мультипликативно оптимальной сигнализирующей ч.и.г. для вычисления f ,

3) не существует такой п.о.р. функции, для вычисления которой h_2 явилась бы сильно аддитивно оптимальной сигнализирующей ч.и.г.

ДОКАЗАТЕЛЬСТВО. Основная идея доказательства состоит в следующем. Пусть известно, что некоторая машина $\mathfrak{M}$ при предельном вычислении какой-то функции для каждого x меняет гипотезу не менее чем a раз. Тогда работу $\mathfrak{M}$ можно моделировать машиной $\mathfrak{M}'$, которая работает таким же образом, но первое выходное значение выдает лишь после того, когда $\mathfrak{M}'$ уже изменила выходное значение a раз. Очевидно, машина $\mathfrak{M}'$ предельно вычисляет ту же функцию, но с меньшей сигнализирующей ч.и.г.

Определяем $h_2(x)$ как наименьшую целую степень числа $^{\rho} x+2$, которая не меньше чем $1+h_1(x)$. Легко видеть, что $h_2(x)$ можно задать с помощью общерекурсивной функции $\tilde{h}(x,n)$ $(h_2(x)=\lim\limits_n \tilde{h}(x,n);\ \tilde{h}(x,n)\leqslant \tilde{h}(x,n+1))$, принимающей в качестве значения только целые степени числа $x+2$. Отметим одну особенность функции $\tilde{h}$, вытекающую из вышеизложенного: если $\tilde{h}(x,n)\neq \tilde{h}(x,n+1)$, то $\tilde{h}(x,n+1)\geqslant \tilde{h}(x,n)$.

Утверждение 1) теоремы теперь очевидно. Докажем утверждение 3). (На самом деле будет доказано более сильное свойство функции h_2. Формулировка этого свойства сложнее утверждения 3) и менее наглядна - поэтому она приведена лишь после доказательства теоремы.)

Через $H_{\mathfrak{M}}(x)$ будем обозначать сигнализирующую ч.и.г. машины $\mathfrak{M}$, работающей на значении аргумента x.

Допустим от противного, что существует такое $\varepsilon>0$ и такая п.о.р. функция $f'(x)$, что:

а) существует машина $\mathfrak{M}$, которая предельно вычисляет $f'(x)$, и для которой для всех x $H_{\mathfrak{M}}(x)\leqslant h_2(x)$,

б) для любой машины $\tilde{\mathfrak{M}}$, которая предельно вычисляет $f'(x)$, для почти всех x $H_{\tilde{\mathfrak{M}}}(x)\geqslant(\frac{1}{2}+\varepsilon)\cdot h_2(x)$.

Из этого допущения, в частности, вытекает, что $\varepsilon<\frac{1}{2}$ и что для почти всех x $H_{\mathfrak{M}}(x)\geqslant(\frac{1}{2}+\varepsilon)\cdot h_2(x)$.

Опишем работу другой машины $\mathfrak{M}'$, которая также предельно вычисляет $f'(x)$, но с меньшей сигнализирующей ч.и.г. Обозначим через A множество всех тех x, при которых либо $H_{\mathfrak{M}}(x)\leqslant(\frac{1}{2}+\varepsilon)\cdot h_2(x)$, либо $\frac{1}{x+2}>\frac{\varepsilon}{2}$. Для всех x из множества A (это множество конечное) машина $\mathfrak{M}'$ с самого начала печатает правильные выходные значения $f'(x)$. Для остальных x машина $\mathfrak{M}'$ моделирует работу $\mathfrak{M}$, не выдавая выходных значений до тех пор, пока для какого-то n_1 не окажется, что число $H_{\mathfrak{M}}(x,n_1)$ изменений гипотезы машиной $\mathfrak{M}$ на x за n_1 тактов больше чем $(\frac{1}{2}+\varepsilon)\cdot\tilde{h}(x,n_1)$. Далее моделирование работы $\mathfrak{M}$ происходит уже с выдачей всех вновь вырабатываемых значений, пока не найдется такое $n' > n_1$, что либо $\tilde{h}(x,n') \neq \tilde{h}(x,n'-1)$, либо $H_{\mathfrak{M}}(x,n') > \tilde{h}(x,n'-1) = \tilde{h}(x,n_1)$. Наступление любого из этих двух событий означает, что $h_2(x) \neq \tilde{h}(x,n_1)$. Следовательно, $h_2(x) \geqslant (x+2)\cdot\tilde{h}(x,n_1)$. После нахождения такого n' машина $\mathfrak{M}'$ моделирует работу $\mathfrak{M}$ без выдачи выходных значений до обнаружения такого n_2, что $H_{\mathfrak{M}}(x,n_2) > \left(\frac{1}{2}+\varepsilon\right)\cdot\tilde{h}(x,n_2)$. Далее моделирование работы $\mathfrak{M}$ происходит уже с выдачей вновь вырабатываемых выходных значений до тех пор, пока не найдется такое $n'' > n_2$, что либо $\tilde{h}(x,n'') \neq \tilde{h}(x,n''-1)$, либо $H_{\mathfrak{M}}(x,n'') > \tilde{h}(x,n''-1) = \tilde{h}(x,n_2)$ и т.д.

Из предположения от противного вытекает, что после такого $n^{(i)}$, при котором $\tilde{h}(x,n^{(i)}) = h_2(x)$, должно найтись такое n_{i+1}, что $H_{\mathfrak{M}}(x,n_{i+1}) > \left(\frac{1}{2}+\varepsilon\right)\tilde{h}(x,n_{i+1}) = \left(\frac{1}{2}+\varepsilon\right)\cdot h_2(x)$. Поэтому $\mathfrak{M}'$, начиная с моделирования такта n_{i+1} работы $\mathfrak{M}$, будет печатать все вновь вырабатываемые машиной $\mathfrak{M}$ выходные значения и, вследствие этого, на данном x предельно вычислит тот же результат, что и машина $\mathfrak{M}$.

Подсчитаем сигнализирующую ч.и.г. $H_{\mathfrak{M}'}(x)$ машины $\mathfrak{M}'$. После моделирования такта n_{i+1} работы $\mathfrak{M}$ машина $\mathfrak{M}'$ делает не более чем $h_2(x) - \left(\frac{1}{2}+\varepsilon\right)\cdot h_2(x)$ изменений выходного значения, между тактами $n^{(i)}$ и n_{i+1} изменений не происходит, а до моделирования такта $n^{(i)}$ может быть сделано не более $\tilde{h}(x,n^{(i)}-1) \leqslant \frac{1}{x+2}\cdot h_2(x) \leqslant \frac{\varepsilon}{2}\cdot h_2(x)$ изменений. Значит, $H_{\mathfrak{M}'}(x) \leqslant \frac{1}{2}\cdot h_2(x)$, что противоречит допущению от противного.

Утверждение 3) доказано. Остается доказать утверждение 2).

Для определения требуемого предиката $f(x)$ будет построена такая общерекурсивная функция $\tilde{f}(x,n)$, что $f(x) = \lim\limits_{n} \tilde{f}(x,n)$. Можно представить себе $\tilde{f}(x,n)$ как n-ое выходное значение некоторой машины $\mathfrak{M}''$, работающей на x .

Для сокращения обозначений сигнализирующую ч.и.г. машины $\mathfrak{M}_i$ на аргументе x будем обозначать просто через $H_i(x)$. Число изменений гипотезы машины $\mathfrak{M}_i$ на аргументе x в течение первых n тактов будем обозначать через $H_i(x,n)$. Через $\mathfrak{M}_i(x,n)$ будем обозначать последнее выходное значение, печатание которого завершено за n тактов работы машины $\mathfrak{M}_i$ на x . (Это значение не определено, если $\mathfrak{M}_i$ на x за n тактов не закончило выдачу ни одного значения, однако по (i,x,n) можно эффективно выяснить, определено ли $\mathfrak{M}_i(x,n)$.) Без ущерба для общности будем считать, что $h_2(x)$ задано в виде предела $h_2(x)=\lim\limits_n \tilde{h}(x,n)$ общерекурсивной функции $\tilde{h}$, монотонной по второму аргументу и принимающей в качестве значений $\tilde{h}(x,n)$ только целые положительные степени числа $x+2$.

Для определения функции $\tilde{f}$ введем вспомогательные функции m , $\tilde{u}$, u : $m(x)$ - это число изменений гипотезы, когда $h_2(x)$ вычисляется при помощи $\tilde{h}$; $\tilde{u}(x,n)=[\sqrt{\tilde{h}(x,n)}]$; $u(x)=\lim\limits_n \tilde{u}(x,n)$. Очевидно, что $u(x)=[\sqrt{h_2(x)}]$.

Существует единая процедура, которая по данным i , x , n дает ответ на вопрос " $H_i(x,n)<[\frac{1}{2^{i+2}}\cdot\tilde{h}(x,n)]$?" Пользуясь этой процедурой, одновременно определяются значения функции $\tilde{f}$ и вспомогательных функций p , g , v . Функции g и v общерекурсивны. Функция $p(x,n)$ частично рекурсивна с рекурсивной областью определения. Она является аналогом функции опровержения в доказательстве теоремы Рабина [6] .

Для всех x $\tilde{f}(x,0)=0$ и $p(x,0)$ не определена. Для всех ℓ,n $g(\ell,n)$ - число таких r , что $p(\ell,r)=p(\ell,r-1)$ & $r<n$. Далее, $v(x,n)=$ $\min\{x-1, [\frac{1}{4}\cdot\tilde{h}(x,n)]$; максимальное y , при котором $\sum\limits_{\ell=0}^{y} g(\ell,n)\le\frac{x}{8}\}$.

Для определения $\tilde{f}(0,n)$ и $p(0,n)$ при $n>0$, узнаем ответ на вопрос "$H_0(0,n)<\left[\frac{1}{4}\cdot\tilde{h}(0,n)\right]$?" Если <u>нет</u>, то $\tilde{f}(0,n)=\tilde{f}(0,n-1)$ и $p(0,n)$ не определена. Если <u>да</u>, то $p(0,n)=0$ и

$$\tilde{f}(0,n)=\begin{cases} f(0,n-1) & \text{, если } \mathfrak{M}_0(0,n) \text{ не определена} \\ \overline{sg}\, \mathfrak{M}_0(0,n) & \text{, если } \mathfrak{M}_0(0,n) \text{ определена.} \end{cases}$$

Для определения $\tilde{f}(x,n)$ и $p(x,n)$ при $x>0$ и $n>0$ составляем список вопросов

$$H_0(x,n)<\left[\frac{1}{2^2}\cdot\tilde{h}(x,n)\right] ? \qquad (0)$$

$$H_1(x,n)<\left[\frac{1}{2^3}\cdot\tilde{h}(x,n)\right] ? \qquad (1)$$

- -

$$H_{\tilde{u}(x,n)}(x,n)<\left[\frac{1}{2^{\tilde{u}(x,n)+2}}\cdot\tilde{h}(x,n)\right] ? \qquad (\tilde{u}(x,n))$$

Из этого списка вычеркиваем вопросы с номерами $(p(0,n)),\ (p(1,n)),\ \ldots,\ (p(v(x,n),n))$, но порядок оставшихся вопросов не меняем.

Если ответы на все оставшиеся вопросы отрицательны, то $p(x,n)$ не определена и $\tilde{f}(x,n)=\tilde{f}(x,n-1)$. Если вопрос (i) является первым в оставшемся после вычеркивания списке, ответ на который положителен, то $p(x,n)=i$ и

$$\tilde{f}(x,n)=\begin{cases} \tilde{f}(x,n-1) & \text{, если } \mathfrak{M}_i(x,n) \text{ не определена} \\ \overline{sg}\, \mathfrak{M}_i(x,n) & \text{, если } \mathfrak{M}_i(x,n) \text{ определена.} \end{cases}$$

Приступим к доказательству сильной мультипликативной оптимальности функции h_2 для вычисления f. Сначала докажем, что существует машина, вычисляющая f

с сигнализирующей ч.и.г., не превосходящей h_2 . Для этого подсчитаем число изменений значений в последовательности $\tilde{f}(x,0), \tilde{f}(x,1), \tilde{f}(x,2), \dots$. Отметим, что если $\tilde{f}(x,n) \neq \tilde{f}(x,n-1)$ и $p(x,n)=p(x,n-1)$, то $\mathfrak{m}_{p(x,n)}(x,n) \neq \mathfrak{m}_{p(x,n)}(x,n-1)$. Сколько может быть таких n при фиксированном x ? Очевидно, не более чем $\frac{1}{2^2}\cdot h_2(x)$ таких n , что $p(x,n)=0$, плюс еще не более чем $\frac{1}{2^3}\cdot h_2(x)$ таких n , что $p(x,n)=1$; плюс еще не более чем $\frac{1}{2^4}\cdot h_2(x)$ таких n , что $p(x,n)=2$ и т.д. Всего, число таких n не превосходит $\frac{1}{2}\cdot h_2(x)$

Остается подсчитать, сколько имеется таких n , что $p(x,n)\neq p(x,n-1)$. Очевидно, при таком n либо $\tilde{h}(x,n)\neq\tilde{h}(x,n-1)$, либо $\tilde{h}(x,n)=\tilde{h}(x,n-1)$ &

& $H_{p(x,n-1)}(x,n) > \left[\frac{1}{2^{p(x,n-1)+2}}\cdot\tilde{h}(x,n)\right]$ & $H_{p(x,n-1)}(x,n-1) \leqslant \left[\frac{1}{2^{p(x,n-1)+2}}\cdot\tilde{h}(x,n-1)\right]$,

либо $\tilde{h}(x,n)=\tilde{h}(x,n-1)$ & $v(x,n) > v(x,n-1)$, либо $\tilde{h}(x,n)=\tilde{h}(x,n-1)$ & $v(x,n)=v(x,n-1)$ &

& $\{p(0,n-1), p(1,n-1), \dots, p(v(x,n-1),n-1)\} \neq \{p(0,n), p(1,n), \dots, p(v(x,n),n)\}$.

Оценим число таких n для каждой из этих четырех возможностей отдельно. Так как каждое значение $\tilde{h}(x,n)$ является целой степенью числа $x+2$, то первая возможность встречается не более чем $m(x) \leqslant \log_{x+2} h_2(x)$ раз, т.е. $o(h_2(x))$ раз. Вторая возможность встречается не более чем $m(x)\cdot u(x) \leqslant \log_{x+2} h_2(x)\cdot\sqrt{h_2(x)} = o(h_2(x))$ раз. Третья возможность встречается не более чем $\lim\limits_{n} v(x,n)$ раз, т.е. не более чем $\frac{1}{4}\cdot h_2(x)$ раз. Четвертая возможность, по определению функции $v(x,n)$, может встречаться не более чем $\frac{x}{8}$ раз, т.е. не более чем $\frac{1}{8}\cdot h_2(x)$ раз.

Итак, существует способ предельного вычисления с сигнализирующей ч.и.г. не превышающей

$\frac{7}{8}\cdot h_2(x)+o(h_2(x))$, т.е. не превышающей $h_2(x)$ для почти всех x . Следовательно, на подходящей другой машине можно предельно вычислить $f(x)$ с сигнализирующей ч.и.г. $h_2(x)$ для всех x .

Теперь докажем, что для каждой машины $\mathfrak{M}_i$, которая предельно вычисляет $f(x)$, существует такое $c>0$, что для почти всех x $H_i(x) \geqslant c\cdot h_2(x)$

Обозначим $\lim\limits_n v(x,n)$ через $v(x)$ и $\lim\limits_n p(x,n)$ через $p(x)$. Если при каком-то x значение $p(x)$ определено, то как легко видеть, машина $\mathfrak{M}_{p(x)}$ не вычисляет предельно $f(x)$. Если же $p(x)$ не определено, то $p(x,n)$ не определено для почти всех n . (Фактически это было доказано выше при подсчете числа изменений значений в последовательности $\tilde{f}(x,0), \tilde{f}(x,1), \tilde{f}(x,2), \ldots$.)

Из неравенств $v(x,n+1)\geqslant v(x,n)$ и $v(x,n)< x-1$, имеющих место для всех x и n , вытекает, что $v(x)$ всюду определена. К тому же $\lim\limits_x v(x)=+\infty$. Это вытекает из $\tilde{h}(x,n)\geqslant x+2$ и существования при любом ℓ предела $\lim\limits_n g(\ell,n)$ (вследствие свойств функции $p(x)$, отмеченных в предыдущем абзаце).

Допустим от противного, что существует машина $\mathfrak{M}_i$ предельно вычисляющая $f(x)$, сигнализирующая ч.и.г. которой при бесконечно многих x меньше, чем

$\left[\frac{1}{2^{i+2}}\cdot h_2(x)\right]$, притом i - наименьший номер такой машины. Пусть x_1 - такое число, что $x_1>(i+1)^2-2$ и

$H_i(x_1)<\left[\frac{1}{2^{i+2}}\cdot h_2(x)\right]$. Пусть n' - настолько большое число, что $\forall j< x_1 \quad \forall n>n' \; (p(j,n)=p(j,n-1))$. Заметим, что отсюда следует $\forall j< x_1 \; \forall n>n' \,(p(j,n)\neq i)$, иначе $\mathfrak{M}_i$ не вычисляла бы f . Так как

$x_1>(i+2)^2-2$, то $\left[\sqrt{x_1+2}\right]>i$, и, следовательно, $\forall x'>x_1 \quad u(x')>i$. Из определения

$p(x_1, n')$ тогда вытекает, что $p(x_1, n')$ определено и принимает значение меньше чем i.

Пусть x_2 - такое число, что $x_2 > x_1$, $v(x_2) > x_1$ и $H_i(x_2) < \left[\frac{1}{2^{i+2}} \cdot h_2(x)\right]$, а n'' -настолько большое, что $\forall j < x_2 \ \forall n \geqslant n'' \ (p(j,n) = p(j,n-1))$. Из определения $p(x_2, n'')$ вытекает, что $p(x_2, n'')$ определено меньше чем i и отлично от $p(x_1, n')$.

Пусть x_3 - такое число, что $x_3 > x_2$, $v(x_3) > x_2$ и $H_i(x_3) < \left[\frac{1}{2^{i+2}} \cdot h_2(x_3)\right]$, а n''' - настолько большое, что $\forall j \leqslant x_3 \ \forall n \geqslant n''' \ (p(j,n) = p(j,n-1))$. Из определения $p(x_3, n''')$ вытекает, что $p(x_3, n''')$ определено меньше чем i и отлично как от $p(x_1, n')$, так и от $p(x_2, n'')$.

Аналогично определяем $x_4, x_5, \ldots$, но после определения x_{i+1} выявляется противоречие, так как числа $p(x_1, n'), p(x_2, n''), \ldots, p(x_{i+1}, n^{(i+1)})$, с одной стороны, попарно различны, а с другой стороны, натуральны и меньше чем i.

Теорема доказана.

Как уже выше было отмечено, приведенное доказательство на самом деле доказывает более общую теорему.

ТЕОРЕМА 1'. Для любой всюду определенной сигнализирующей ч.и.г. h_1 существует такая п.о.р. функция h_2 что:

1) для всех x $h_1(x) \leqslant h_2(x) \leqslant (2+x)(1+h_1(x))$,

2) существует такой п.о.р. предикат f, что h_2 является сильно мультипликативно оптимальной сигнализирующей ч.и.г. для вычисления f,

3) если h_2 является сильно оптимальной сигнализирующей ч.и.г. с точностью до некоторого семейства $\{g_i(y)\}$ для предельного вычисления какой-то п.о.р. функции, то для каждого $\varepsilon > 0$ семейство $\{g_i(y)\}$ содержит функцию $g_i(y)$ которая для бесконечно многих y не превосходит $\left(\frac{1}{2}+\varepsilon\right) \cdot y$.

ЛИТЕРАТУРА

1. Gold E.M. Limiting recursion.-"Journal of Symbolic Logic", 1965, v. 30, No 1.
2. Putnam H. Trial and error predicates and the solution to a problem of Mostowski.-"Journal of Symbolic Logic", 1965, v. 30, No 1.
3. Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. М., 1972.
4. Фрейвалд Р.В. Предельно вычислимые функции и функционалы.-"Уч.зап.Латв. ун-та", 1974. .210.
5. Блюм М. Машинно-независимая теория сложности рекурсивных функций.-В кн.: Проблемы математической логики. М., 1970.
6. Трахтенброт Б.А. Сложность алгоритмов и вычислений. Новосибирск, 1967.
7. Ходжаев Дж. О сложности вычислений на машинах Тьюринга с оракулом.-Кандидатская диссертация. Ташкент, 1970.
8. Rabin M.O. Speed of computation of functions and classification of recursive sets.-"Bull.Rec.Counc.of Israel", 8F, 1959.
9. Borodin A. Computational complexity and the existence of comlexity gaps.-"Journal of the Association for Computing Machinery", 1972, v.19, No 1.
10. Young P. Easy constructions in complexity theory: gap and speed-up theorems.-"Proceedings of the American Mathematical Society", 1973, v.37, No 2.
11. Barzdin J.M. Prognostication of automata and functions.-Information Processing 71. North-Holland, 1972.
12. Барздинь Я.М., Фрейвалд Р.В. Прогнозирование общерекурсивных функций - ДАН СССР, 1972, т.206, № 3.

О ЧАСТОТНЫХ ВЫЧИСЛЕНИЯХ В РЕАЛЬНОЕ ВРЕМЯ

Е.Б.Кинбер

В настоящей работе изучается следующий вопрос: можно ли в реальное время с относительно высокой частотой вычислять предикаты, которые в обычном смысле в реальное время не вычислимы. Этот вопрос был предложен автору Б.А.Трахтенбротом.

Наш результат заключается в следующем: существуют сколь угодно сложные (в смысле времени вычисления) предикаты, которые с относительно высокой частотой вычислимы в реальное время. Отсюда, в частности, следует положительный ответ на вопрос Б.А.Трахтенброта.

В работе используется формализация частотных вычислений, рассмотренная в [2], [3], [4].

ОПРЕДЕЛЕНИЕ 1. Будем говорить, что предикат $\varphi(x)(m,n)$ – вычислим $(m \leq n)$ оператором T, если каждой n-ке натуральных чисел $(x_1, x_2, \dots, x_n)$, где $x_i \neq x_j$, $i \neq j$, оператор T сопоставляет такую n-ку нулей и единиц $(y_1, y_2, \dots, y_n)$, что среди равенств

$$\varphi(x_1)=y_1,\ \varphi(x_2)=y_2,\ \dots,\ \varphi(x_n)=y_n$$

по крайней мере m истины.

Наша модель (m,n) – вычислений в реальное время является некоторым видоизменением обычной модели вычислений в реальное время, рассмотренной, например, в [5] и [6]. Для вычислений используется многоленточная машина Тьюринга $\mathfrak{M}$ с входным алфавитом Σ', конечным множеством состояний S, рабочим алфавитом W и выходным алфавитом $\{0,1\}$. Один из символов $\Lambda \in \Sigma'$ специально выделен (т.н. пустой символ). Выделено также начальное состояние s_0. На каждой из лент имеется одна головка, которая может читать и писать. Машина $\mathfrak{M}$ имеет n входов и n выходов. В каждый момент на каждый из входов машины $\mathfrak{M}$ поступает по одному символу из Σ' и на каждом из выходов выдается символ из $\{0,1\}$.

Множество всех конечных слов в произвольном алфавите R обозначается через R^*. Произвольное слово из R^* будем называть R-словом. Обозначим через Σ множество $\Sigma' \setminus \{\Lambda\}$.

Пусть $(x_1, x_2, \dots, x_n)$ - произвольная n-ка попарно различных Σ-слов. Рассматривая для такой n-ки n-ку слов $(\Lambda^{i_1} x_1, \Lambda^{i_2} x_2, \dots, \Lambda^{i_n} x_n)$, мы всегда будем предполагать, что слова $\Lambda^{i_1} x_1, \Lambda^{i_2} x_2, \dots, \Lambda^{i_n} x_n$ имеют одинаковую длину.

ОПРЕДЕЛЕНИЕ 2. Пусть φ_M - характеристическая функция некоторого множества $M \subseteq \Sigma^*$. Говорят, что множество M (m, n) - распознаваемо в реальное время, если в момент завершения подачи произвольной n-ки $(\Lambda^{i_1} x_1, \dots, \Lambda^{i_n} x_n)$, где $x_i \neq x_j,\ i \neq j,\ x_i \in \Sigma^*$, на входы находящейся в состоянии s_0 и при пустых рабочих лентах некоторой машины $\mathfrak{M}$ на выходах $\mathfrak{M}$ выдается такая n-ка символов $(\alpha_1, \alpha_2, \dots, \alpha_n)$, что среди равенств

$$\varphi(x_1) = \alpha_1,\ \varphi(x_2) = \alpha_2,\ \dots,\ \varphi(x_n) = \alpha_n$$

по крайней мере m истинны.

"Пустые" слова Λ^{i_k} добавляются к x_k, чтобы функцию φ_M можно было вычислять на n-ках слов различной длины.

Как и в [1], через $t_{\mathfrak{A}}(x)$ обозначается сигнализирующая времени работы машины Тьюринга $\mathfrak{A}$ на слове x . Через $|x|$ условимся обозначать длину слова x . $\forall_x^\infty$ означает "для всех x за исключением, быть может, конечного числа", соответственно, $\exists_x^\infty$ -"для бесконечно многих x ".

ТЕОРЕМА. Для любой общерекурсивной функции (о.р.ф.) $T(x)$ и для любого $n \geqslant 2$ существует такое множество M , что 1) M $(n-1, n)$ -распознаваемо в реальное время;

2) для любой (однолентной) машины Тьюринга $\mathfrak{A}$, распознающей M в обычном смысле:

$$\exists_z^\infty (t_{\mathfrak{A}}(z) \geqslant T(z))$$

ДОКАЗАТЕЛЬСТВО. Пусть $\nu(x)$ - произвольная о.р.ф. По теореме Рабина [1] существует множество A слов в некотором алфавите U такое, что для любой машины $\mathfrak{A}$, распознающей A ,

$$\forall_x^\infty (t_{\mathfrak{A}}(x) \geqslant \nu(x)).$$

Известно также, что A можно выбрать таким образом, чтобы оно было распознаваемо за время $t(x) = \nu^2(x)$.

Добавим к алфавиту U символы $0, 1, \alpha, \gamma, *$ (предполагается, что эти символы не содержатся в U). Пусть u_i - i -ое в лексикографическом порядке U -слово и μ_i -значение на u_i φ_A - характеристической функции множества A . Элементы требуемого множества $M = M_\nu$ определяются по индукции:

$$a_1 = u_1\, \mu_1\, \gamma ;$$

пусть a_k уже определено, $a_k = b\gamma$ и u_i -максимальное в лексикографическом порядке U - подслово слова a_k ; мы полагаем

$$a_{k+1} = b\alpha\, u_{i+1} \mu_{i+1} {}^* u_{i+2} \mu_{i+2} {}^* \ldots {}^* u_r \mu_r \gamma ,$$

где: 1) длина слова $u_{i+1} \mu_{i+1} {}^* \ldots {}^* u_r \mu_r \gamma$ не меньше числа $2 \sum_{j=1}^{i} \nu^2(u_j)$;

2) a_{k+1} имеет наименьшую длину среди слов, удовлетворяющих условию 1).

В множество M_ν заносятся слова $a_1, \dots, a_k, a_{k+1} \dots$, в его дополнение $\bar{M}_\nu$ - все остальные слова в алфавите $U \cup \{0,1,\alpha,\gamma\}$.

Выберем теперь функцию $\nu(x)$ таким образом, чтобы выполнялись условия:

а) $\lim\limits_{|x|\to\infty} \frac{|x|^2}{\nu(x)} = 0$

б) $\forall k [2 \sum\limits_{i=1}^{k} \nu^2(u_i) \geqslant (k+1)(2+2\sum\limits_{i=1}^{k}(2+|u_i|)]$.

Заметим, что для любого p $|a_p| \leqslant \sum\limits_{i}^{r(p)}(2+|u_i|)$, , где $u_{r(p)}$ -максимальное в лексикографическом порядке U -подслово в a_p . Следовательно, имеет место

б)' $\forall p [2 \sum\limits_{i=1}^{r(p)} \nu^2(u_i) \geqslant (r(p)+1)(2|a_p|+2)]$

ЛЕММА. Если $n \geqslant 2$ и функция $\nu(x)$ удовлетворяет условиям (а) и (б), то множество M_ν $(n-1,n)$ -распознаваемо в реальное время.

ДОКАЗАТЕЛЬСТВО. Машина $\mathfrak{M}$, $(n-1,n)$ -распознающая M_ν , имеет входной алфавит $\Sigma' = \Sigma \cup \{\lambda\}$, где $\Sigma = U \cup \{0,1,\alpha,\gamma,{}^*\}$, рабочий алфавит $W \supseteq \Sigma$, $3\sum\limits_{k=1}^{n-1} k$ рабочих лент; множество всех лент делится на группы по три ленты, каждая из которых соответствует одной из пар (i,j) входов $(1 \leqslant i < j \leqslant n)$ машины $\mathfrak{M}$.

Опишем действия $\mathfrak{M}$ на тройке лент, соответствующей паре (j,k) , когда на входы поступает n -ка попарно различных слов $(\lambda^{i_1}x_1, \lambda^{i_2}x_2, \dots, \lambda^{i_n}x_n)$.

Предположим сначала, что $|x_j| > |x_k|$. По мере поступления на j -й вход слова x_j вплоть до появления на k -ом входе первого символа слова x_k машина $\mathfrak{M}$ совершает следующие действия:

1. На первой из лент, соответствующих паре (j,k), $\mathfrak{M}$ записывает x_j.

2. На второй из этих лент $\mathfrak{M}$ выясняет, содержатся ли в M_ν слова $w_1\gamma, w_2\gamma, \ldots, w_r\gamma$, ... , где $w_i\alpha$ - i -й по длине начальный фрагмент слова x_j, заканчивающийся на α; это выяснение происходит сначала для $w_1\gamma$, затем для $w_2\gamma$ и т.д. Основное время при этом затрачивается, очевидно, на проверку следующих двух обстоятельств:

L 1) U -подслова в слове $w_i\gamma$ расположены в лексикографическом порядке;

L 2) символы, следующие за U - подсловами, являются значениями φ_A на этих подсловах.

Условие L 1 проверяется за время порядка $\sum_{r=1}^{p}|u_r|^2$, где u_p -максимальное в лексикографическом порядке U - подслово в $w_i\gamma$. В силу (а) это время по порядку меньше, чем $\sum_{r=1}^{p}\nu(u_r)$. Условие L 1 в силу нашего предположения можно проверить за время $\sum_{r=1}^{p}\nu^2(u_r)+O(\sum_{r=1}^{p}\nu^2(u_r))$.

Отсюда легко следует, что принадлежность слова $w_i\gamma$ множеству M_ν можно установить за время $2\sum_{r=1}^{p}\nu^2(u_r)$.

Мы будем предполагать, что время работы $\mathfrak{M}$ на каждом $w_i\gamma$ равно в точности $2\sum_{r=1}^{p}\nu^2(u_r)$.

L 3) На третьей ленте $\mathfrak{M}$ сначала записывает слово $w_1\gamma$ и возвращает головку к ячейке, содержащей передний символ $w_1\gamma$; затем, когда на второй ленте заканчиваются вычисления, связанные с $w_i\gamma$, $\mathfrak{M}$ начинает записывать на третьей ленте вместо $w_1\gamma$ слово $w_2\gamma$ и, закончив, снова возвращает головку к ячейке, содержащей первый символ $w_2\gamma$. Далее, когда на второй ленте заканчиваются вычисления, связанные с $w_2\gamma$, $\mathfrak{M}$ начинает записывать вместо $w_2\gamma$ слово $w_3\gamma$ и по окончании возвращает головку к ячейке, содержащей первый символ $w_3\gamma$ и т.д. Если в ходе вычислений на второй ленте на некотором шаге выясняется, что $w_i\gamma \notin M_\nu$

то действия $\mathfrak{M}$ на третьей ленте немедленно прекращаются.

С момента появления на входе первого символа слова x_k $\mathfrak{M}$ начинает сравнивать на совпадение x_k и слово, записанное к этому моменту на третьей ленте справа от головки (включая символ, обозреваемый головкой).

Если $|x_j| \leq |x_k|$, то $\mathfrak{M}$ работает аналогичным образом, но при этом x_j и x_k меняются ролями.

Опишем теперь, какой будет n-ка $(\sigma_1, \ldots, \sigma_n)$ символов на выходах $\mathfrak{M}$ после подачи на входы произвольной n-ки слов $(\Lambda^{i_1} x_1, \Lambda^{i_2} x_2, \ldots, \Lambda^{i_n} x_n)$. Для любого j $\sigma_j = 1$ в том и только в том случае, когда существует такое $r \neq j$, $1 \leq r \leq n$, для которого выполняются следующие условия:

N 1) К моменту поступления на вход первого символа слова x_j на третьей ленте, соответствущей паре (j,r) в ячейке слева от головки находится пустой символ.

N 2) $|x_r| > |x_j|$

N 3) x_j совпадает со словом, записанным на третьей ленте, соответствующей (j,r) ; оба слова заканчиваются символом γ .

N 4) К моменту окончания подачи на входы рассматриваемой n-ки в ходе вычислений на второй ленте, соответствующей (j,r) , выяснено, что x_j содержится в M_φ .

Покажем, что $\mathfrak{M}$ $(n-1, n)$-распознает M_φ . Пусть $(\Lambda^{i_1} x_1, \Lambda^{i_2} x_2, \ldots, \Lambda^{i_n} x_n)$ - произвольная n-ка, в которой $x_i \neq x_j$, $i \neq j$ и $(\sigma_1, \sigma_2, \ldots, \sigma_n)$ - n-ка символов, которые $\mathfrak{M}$ выдает на выходах после подачи $(\Lambda^{i_1} x_1, \Lambda^{i_2} x_2, \ldots, \Lambda^{i_n} x_n)$. Достаточно показать, что для любых r и j , где $r \neq j$, по крайней мере одно из равенств $\varphi_{M_\varphi}(x_j) = \sigma_j$ или $\varphi_{M_\varphi}(x_r) = \sigma_r$ истинно. Заметим, что если $x_k \notin M_\varphi$, то в силу N 4 σ_k не может быть равно единице. Таким образом, остается проверить, что при $x_r \in M_\varphi$ и $x_j \in M_\varphi$ σ_r и σ_j не могут быть одновременно равны нулю.

Из определения M_ν легко следует, что $x_r, x_j \in M_\nu$ не могут иметь одинаковую длину. Пусть, например, $|x_j| > |x_r|$ и пусть u_k - максимальное в лексикографическом порядке U -подслово в x_r. Слово x_r получается, очевидно, заменой в некотором подслове $w\alpha$ слова x_j символа α на γ. На второй ленте, соответствующей паре (r,j), машина $\mathfrak{M}$ в точности за $2\sum\limits_{i=1}^{k} \nu^2(u_i)$ тактов выясняет, что $w\gamma = x_r \in M_\nu$. Одновременно на третьей ленте, соответствующей (r,j), $\mathfrak{M}$ не более чем за $k(2|x_r|+2)$ тактов записывает x_r и возвращает головку к ячейке, содержащей первый символ в x_r. Так как в силу (б)' $2\sum\limits_{i=1}^{k} \nu^2(u_i) \geq |x_r| + k(2|x_r|+2)$, то к моменту подачи на вход первого символа x_r, головка на третьей ленте уже будет обозревать первый символ слова $w\gamma$. Поэтому, сравнивая записанное на третьей ленте слово $w\gamma$ и поступающее на вход слово x_r, машина $\mathfrak{M}$ обнаружит их совпадение. В таком случае после окончания подачи слова x_r на r -ом выходе будет выдана единица. Лемма доказана.

Для произвольной машины $\mathcal{B}$, следуя [1], введем следующее обозначение:

$$t_{\mathcal{B}}(k) = \max_{|x|=k} t_{\mathcal{B}}(x)$$

Пусть z - произвольное слово из M_ν и $x(z)$ -максимальное в лексикографическом порядке U -подслово в z. Достаточно просто убедиться в том, что исходное множество A можно распознавать на некоторой машине $\mathfrak{A}$ таким образом, чтобы для указанных z и $x(z)$ выполнялось неравенство

$$(*)\quad t_{\mathfrak{A}}(x(z)) \leq 2^{cz^{|x(z)|+1}}\, t_{\mathfrak{N}}(|z|)$$

где $\mathfrak{N}$ -некоторая машина Тьюринга, распознающая M_ν, а c - константа, не зависящая от $\mathfrak{A}$, $\mathfrak{N}$, z. Мы коротко опишем, как работает такая машина $\mathfrak{A}$ на произвольном U -слове $x = u_i$.

Сначала $\mathfrak{A}$ записывает на ленте в лексикографическом порядке слова $u_1, u_2, \dots, u_i$, разделяя их двумя пустыми ячейками. В конце полученной записи ставится символ γ . В результате на ленте получится следующее слово

	↓			↓			↓				
u_1	Λ	Λ	u_2	Λ	Λ	— — — —	Λ	Λ	x	Λ	γ

Далее $\mathfrak{A}$ всевозможными способами расставляет символы 0 и 1 в левых пустых ячейках (на рисунке они отмечены стрелками) и символы α и $*$ в правых пустых ячейках. На получающихся таким образом $\sum$ -словах $\mathfrak{A}$ моделирует работу машины $\mathfrak{N}_i$, распознающей M_ν . Если для какого-нибудь из этих $\sum$ - слов выяснится, что оно содержится в M_ν , то для нахождения $\varphi_\Lambda(x)$ нужно прочитать символ, который находится в данном слове справа от U -подслова x . Если ни одно из указанных $\sum$ -слов в M_ν не содержится, то все описанные выше действия машины $\mathfrak{A}$ повторяются для лексикографической последовательности слов $u_1, u_2, \dots, u_i, u_{i+1}$ (напомним, что $x = u_i$) и т.д. до тех пор, пока не будет найдено $\sum$ -слово из M_ν . Неравенство $(*)$ легко можно получить из описания $\mathfrak{A}$.

Пользуясь $(*)$ и условием $\forall x^\infty (t_{\mathfrak{A}}(x) > \nu(x))$, для любой о.р.ф. $T(z)$ можно подобрать столь быстро растущую о.р.ф. $\nu(x)$, чтобы для каждой машины $\mathfrak{N}$ распознающей M_ν , выполнялось условие

$$\exists z^\infty (T(z) \leqslant t_{\mathfrak{N}}(|z|))$$

При этом, очевидно, легко добиться выполнения для $\nu(x)$ условий (а) и (б). Отсюда следует справедливость второго утверждения теоремы.

ЗАМЕЧАНИЕ 1. Остается открытым вопрос о том, можно ли в формулировке теоремы заменить

$$\exists z^{\infty} (t_{\mathcal{R}} (z) > T(z))$$

на

$$\forall z^{\infty} (t_{\mathcal{R}} (z) > T(z)).$$

ЗАМЕЧАНИЕ 2. В рассмотренной нами модели (m, n) - вычислений в реальное время до подачи слова в алфавите Σ на вход машины поступают пустые символы. Можно рассматривать и несколько более общую модель, когда пустые символы могут как угодно располагаться между символами Σ -слова (а также до и после слова). Доказательство теоремы в этом случае отличается лишь некоторыми техническими деталями.

Автор выражает благодарность Р.В.Фрейвалду за ценное обсуждение.

ЛИТЕРАТУРА

1. Трахтенброт Б.А.Сложность алгоритмов и вычислений. Новосибирск, 1967.
2. Трахтенброт Б.А. Частотные вычисления-"Труды Мат.ин-та им.В.А.Стеклова АН СССР",1973, т.113.
3. Трахтенброт Б.А. О частотном вычислении функции.- "Алгебра и логика",1963,т.2, № 1.
4. Кинбер Е.Б. Частотные вычисления общерекурсивных предикатов и частотное перечисление множеств.ДАН СССР,1972, т.205, № 1.
5. Рабин М. Вычисления в реальное время. - В кн.: Проблемы математической логики. М., 1970.
6. Hartmanis J. Stearns R.E.On the computational complexity of algorithms.-Trans.Amer.Math.Soc,1965,11,No 5.

УНИВЕРСАЛЬНЫЕ АВТОМАТЫ БУХБЕРГЕРА И ВЫЧИСЛЕНИЯ В РЕАЛЬНОЕ ВРЕМЯ

М.И.Аугустон

Понятие алгоритма формализуется многими способами. Часто используется язык машин Тьюринга, машин Поста, нормальных алгоритмов Маркова. Все эти и многие другие конструкции имеют существенные общие черты. Исходные данные перед обработкой алгоритмом обычно кодируются, а выходные (если они получены) декодируются. Сам процесс обработки состоит из последовательных шагов применения определенных правил (программы) к результату, полученному на предыдущем шаге. На каждом шаге проверяется, не следует ли закончить процесс вычисления. Если следующий шаг не нужен, то результат декодируется и выдается. Если число шагов бесконечно, то алгоритм на данном входе не определен и не выдается никакого результата. Это общая схема, которой подчиняется любая известная концепция алгоритма. Различные формализации отличаются выбором конкретных кодирующих и декодирующих функций, допустимых программ и критерия остановки.

В [1] Бухбергер списал автоматы, для которых эти четыре основных компонента задаются в наиболее общем виде. Автомат Бухбергера - это четверка $B=\{\gamma, \psi, \kappa, \rho\}$, где γ, ψ, ρ - всюду определенные функции, а κ - всюду определенный предикат. На вход подается аргумент x, он кодируется функцией $\gamma(x)$, к полученному результату применяется итерация ψ : $\psi(\gamma(x))$, $\psi(\psi(\gamma(x)))$, ... (дальше будем применять обозначение $\psi^{(i)}$ для итерации ψ, т.е. $\psi(x) = \psi^{(1)}(x)$, $\psi(\psi(x)) = \psi^{(2)}(x)$ и т.д.).

К каждому результату итерации применяется предикат остановки κ, если $\kappa(\psi^{(t)}(\gamma(x)))=0$, то итерация прекращается и результат декодируется функцией ρ. На выход выдается $\rho(\psi^{(t)}(\gamma(x)))$. Этот результат будем обозначать $B(x)$.

Число итераций или число шагов, сделанных автоматом B на входе x будем обозначать $T_B(x)$. Если на входе x процесс итерации не обрывается, будем считать $T_B(x)=\infty$.

Будем называть автомат Бухбергера общерекурсивным (о.р.), если $\gamma, \psi, \kappa, \rho$ - общерекурсивные функции, и будем называть его примитивнорекурсивным (п.р.), если $\gamma, \psi, \kappa, \rho$ - примитивнорекурсивные функции.

Будем обозначать через $\langle m,n\rangle$ канторовский номер пары (m,n) и через $\tau_1 x$ и $\tau_2 x$ проекции этой нумерации пар (см., например, [2]). Используем также функцию $Sgn(x)=0$, если $x=0$, 1 если $x>0$ и $\overline{Sgn}(x)=1-Sgn(x)$.

Пусть $\mathfrak{A}$ некоторый класс автоматов Бухбергера. Автомат U назовем универсальным для класса $\mathfrak{A}$, если

1) $\forall B \in \mathfrak{A} \exists n \; \forall x \; U(\langle n,x\rangle)=B(x)$

и 2) $\forall n \; \exists B \in \mathfrak{A} \; \forall x \; U(\langle n,x\rangle)=B(x)$

n можно считать "программой", по которой обрабатывается аргумент x.

Из теоремы Клини о нормальной форме следует, что любую ч.р. функцию можно вычислять на подходящем автомате Бухбергера, причем даже на примитивнорекурсивном. Таким образом имеет место

ТЕОРЕМА 1. Класс о.р. автоматов имеет п.р. универсальный автомат.

Так как класс п.р. функций имеет универсальную общерекурсивную функцию, то справедлива

ТЕОРЕМА 2. Класс п.р. автоматов имеет п.р. универсальный автомат.

Универсальный автомат U моделирует автоматы из класса $\mathfrak{A}$ в реальное время, если

$$\forall B \in \mathfrak{A}\, \exists c\, \exists n\ \forall x \left\{ U(\langle n,x \rangle) = B(x) \,\&\, T_U(\langle n,x \rangle) \leqslant c \cdot T_B(x) \right\}$$

Из существования для класса п.р.ф. универсальной о.р. функции следует

ТЕОРЕМА 3. Для класса п.р. автоматов существует о.р. универсальный автомат, моделирующий в реальное время.

Причем моделировать любой п.р. автомат можно даже при $c = 1$.

Основной целью настоящей работы является доказательство двух утверждений:

ТЕОРЕМА 4. Не существует универсального о.р. автомата, моделирующего в реальное время класс о.р. автоматов.

ТЕОРЕМА 5. Не существует универсального п.р. автомата, моделирующего в реальное время класс п.р. автоматов.

Доказательства обеих теорем аналогичны. Сначала будем доказывать теорему 4. В дальнейшем, если не оговорено противное, речь идет об о.р. автоматах.

Для доказательства потребуется

ЛЕММА ОБ УСКОРЕНИИ. Для каждого автомата B_1 существует автомат B_2 такой, что

$$\forall x \left\{ B_1(x) = B_2(x) \;\&\; T_{B_2}(x) \leqslant \max\left\{ 1, \log_2 T_{B_1}(x) \right\} \right\}.$$

ДОКАЗАТЕЛЬСТВО. Пусть автомат B_1 задан четверкой $B_1 = \{\gamma_1, \psi_1, \kappa_1, \rho_1\}$. Построим автомат $B_2 = \{\gamma_2, \psi_2, \kappa_2, \rho_2\}$ следующим образом:

$$\gamma_2(x) = \langle 0, x \rangle$$

$$\psi_2(\langle n, x \rangle) = \langle n+1, x \rangle$$

$$\kappa_2(\langle n, x \rangle) = \prod_{i \leqslant 2^{n+1}} \kappa_1(\psi_1^{(i)}(x))$$

$$\rho_2(\langle n, x \rangle) = \sum_{i \leqslant 2^{n+1}} \Big[\overline{sgn}(\kappa_1(\psi_1^{(i)}(x))) \cdot \rho_1(\psi_1^{(i)}(x)) \cdot$$

$$\cdot \overline{sgn}\Big(\sum_{j \leqslant i} \overline{sgn}(\kappa_1(\psi_1^{(j)}(x))) \dot{-} \overline{sgn}(\kappa_1(\psi_1^{(i)}(x)))\Big)\Big].$$

Нетрудно убедиться, что лемма об ускорении допускает обобщение. Вместо $\log$ может быть взята другая вычислимая функция. Так что автоматы Бухбергера можно ускорять в широких пределах. Любое вычисление может быть ускорено на подходящем автомате.

ДОКАЗАТЕЛЬСТВО теоремы 4.

Допустим, существует $U = \{\gamma, \psi, \kappa, \rho\}$ универсальный автомат, моделирующий класс о.р. автоматов в реальное время. Построим автомат $U_1 = \{\gamma_1, \psi_1, \kappa_1, \rho_1\}$ со следующими свойствами:

1) $U_1(\langle 2n, x \rangle) = U(\langle n, x \rangle)$ и $T_{U_1} = T_U$,

2) $U_1(\langle 2n+1, x \rangle) = 0$ и $T_{U_1} = n$,

причем положим $T_{U_1}(\langle 1, x \rangle) = 1$.

Второе условие гарантирует существование программ, на которых U_1 работает долго.

Опишем U_1 точнее:

$$\gamma_1(\langle n,x\rangle) = \begin{cases} \langle n, \gamma(\langle \frac{n}{2}, x\rangle) & n \text{ - четное} \\ \langle n, x\rangle & n \text{ - нечетное} \end{cases}$$

$$\psi_1(\langle n,x\rangle) = \begin{cases} \langle n, \psi(x)\rangle & n \text{ - четное} \\ \langle n \dot{-} 2 + \overline{sgn}(n \dot{-} 2), x\rangle & n \text{ - нечетное} \end{cases}$$

$$\kappa_1(\langle n,x\rangle) = \begin{cases} 0 & n=1 \\ 1 & n \neq 1 \quad \text{и} \quad n \text{ - нечетное} \\ \kappa(x) & n \text{ - четное} \end{cases}$$

$$\rho_1(\langle n,x\rangle) = \begin{cases} 0 & n=1 \\ \rho(x) & \text{для остальных } n \end{cases}$$

U_1 тоже универсальный автомат и моделирует в реальное время. По лемме об ускорении существует автомат U_2 такой, что

$$\forall x [\, U_2(x) = U_1(x) \;\&\; T_{U_2}(x) \leq max\{1, \log_2 T_{U_1}(x)\}],$$

Построим автомат $A = \{\gamma_A, \psi_A, \kappa_A, \rho_A\}$ со следующими свойствами.

Берем два экземпляра автомата U_2 и запускаем их параллельно один на входе $\langle \tau_1 x, x\rangle$, другой на $\langle \tau_2 x, x\rangle$. За один шаг работы А будем моделировать один шаг работы U_2. Пусть первым остановился $U_2(\langle \tau_i x, x\rangle)$, тогда полагаем $A(x) = U_2(\langle \tau_i x, x\rangle) + 1$.
В случае одновременной остановки берем

$$A(x) = U_2(\langle \tau_1 x, x\rangle) + 1,$$

Если ни один из них не остановится, то и $A(x)$ не определен.

Так как за один шаг работы А моделируется один шаг U_2, то число шагов A будет удовлетворять соотношению

$$T_A(x)=\min\{T_{U_2}(\langle \tau_1 x,x\rangle),\ T_{U_2}(\langle \tau_2 x, x\rangle)\}$$
$$\leqslant \min\{\log_2 T_{U_1}(\langle \tau_1 x,x\rangle),\ \log_2 T_{U_1}(\langle \tau_2 x,x\rangle)\}+1 \qquad (1)$$

Опишем автомат A подробно.

$$\gamma_A(x)=\langle \gamma_2(\langle \tau_1 x,x\rangle),\ \gamma_2(\langle \tau_2 x,x\rangle)\rangle$$
$$\psi_A(\langle m,n\rangle)=\langle \psi_2(m),\ \psi_2(n)\rangle$$
$$\kappa_A(\langle m,n\rangle)=\kappa_2(m)\cdot \kappa_2(n)$$
$$\rho_A(\langle m,n\rangle)=\overline{sgn}(\kappa_2(m))\cdot \rho_2(m)+$$
$$+\overline{sgn}(\kappa_2(n))\cdot \rho_2(n)\cdot \kappa_2(m)+1$$

Так как U_1 универсальный автомат, то

$$\exists p_0\ \exists c\ \forall x\{U_1(\langle p_0,x\rangle)=A(x)\ \&\ T_{U_1}(\langle p_0,x\rangle)\leqslant c\cdot T_A(x)\}$$

Для всех x таких, что $\tau_1 x=p_0$ или $\tau_2 x=p_0$ будет верно

$$T_{U_1}(\langle p_0,x\rangle)\leqslant c\cdot T_A(x)\leqslant c\cdot \log_2 T_{U_1}(\langle p_0,x\rangle) \qquad (2)$$

Таких X бесконечно много.

$$\exists^{\infty} x\ T_{U_1}(\langle p_0,x\rangle)\leqslant c\cdot \log_2 T_{U_1}(\langle p_0,x\rangle) \qquad (3)$$

Покажем, что для всех этих x $T_{U_1}(\langle p_0,x\rangle)$ не может быть ограничено константой, этим самым (3) становится противоречивым и предложение доказано.

Допустим, что существует константа M такая, что для всех x таких, что $\tau_1 x=p_0$ или $\tau_2 x=p_0$, выполняется

$$T_{U_1}(\langle p_0, x\rangle) < M. \qquad (4)$$

Рассмотрим пару $(p_0, 2M+3)$. По построению,

$$\forall x \; T_{U_1}(\langle 2M+3, x\rangle) = M+1 \quad ,$$

$T_A(\langle p_0, 2M+3\rangle)$ определено, т.к. $U_1(\langle 2M+3, \langle p_0, 2M+3\rangle\rangle)$ определено. $U_1(\langle p_0, \langle p_0, 2M+3\rangle\rangle)$ тоже определено, т.к. U_1 универсальный автомат.

$$U_1(\langle p_0, \langle p_0, 2M+3\rangle\rangle) = A(\langle p_0, 2M+3\rangle). \qquad (5)$$

Но $U_1(\langle 2M+3, \langle p_0, 2M+3\rangle\rangle)$ останавливается раньше, чем $U_1(\langle p_0, \langle p_0, 2M+3\rangle\rangle)$, т.к. в противном случае имеем

$$A(\langle p_0, 2M+3\rangle) = U_1(\langle p_0, \langle p_0, 2M+3\rangle\rangle) + 1, \qquad (6)$$

что противоречит (5).

Поскольку $U_1(\langle 2M+3, \langle p_0, 2M+3\rangle\rangle)$ останавливается раньше, то

$$T_{U_1}(\langle p_0, \langle p_0, 2M+3\rangle\rangle) > T_{U_1}(\langle 2M+3, \langle p_0, 2M+3\rangle\rangle) = M+1,$$

т.е. $T_{U_1}(\langle p_0, \langle p_0, 2M+3\rangle\rangle) > M+1,$

что противоречит (4). Теорема 4 доказана.

Поскольку все построения в доказательствах леммы об ускорении и самого предложения сохраняют примитивную рекурсивность, эти доказательтва сохраняют силу для теоремы 5.

Автор выражает благодарность Я.М.Барздиню за постановку проблемы, а также другим участникам семинара по теории алгоритмов за внимание к работе.

ЛИТЕРАТУРА

1. Buchberger E. Certain decompositions of Gödel numberings and the semantics of programming languages.- International Symposium on Theoretical Programming. Springer-Verlag. Berlin et al, 1974.

2. Мальцев А.И. Алгоритмы и рекурсивные функции.М.,1965.

ТЕОРЕМА О ДВОЙНОЙ НЕПОЛНОТЕ

К.М.Подниекс

1. Идея изучать теорию-объект в формализованной метатеории принадлежит, по-видимому, П.Лоренцену (см.[I]). Интересное применение этой идеи демонстрирует А.Мостовский [2] : изучение теории множеств ZF (как объекта) в теории классов Морса.

В настоящей статье формализованные метатеории рассматриваются со стороны их неполноты. В метатеории, которая сильнее теории-объекта, иногда можно доказать непротиворечивость последней, но ни в одной фиксированной метатеории нельзя доказать неразрешимость всех "действительно" неразрешимых предложений (достаточно сильной) теории-объекта. С точки зрения такой метатеории можно различить четыре типа предложений теории-объекта: доказуемые, опровержимые, "доказуемо неразрешимые" и "недоказуемо неразрешимые". С точки зрения обычной интуитивной метатеории последние два типа совпадают. Все дело в том, что множество всех неразрешимых предложений, как правило, не является рекурсивно перечислимым.

Как известно, неразрешимую формулу Геделя можно рассматривать как модель классической антиномии Лжец.

$p : p$ ложно

Предложение p , утверждающее собственную ложность, заставляет прибавить к модусам "истинно-ложно" третий модус: "не имеет значения истинности", "неопределено", "неразрешимо". Введение нового модуса исключает обычные антиномии, но приводит к появлению новых.

q : q ложно или q не имеет значения истинности. Это т.н. Усиленный Лжец, здесь: q истинно влечет q ложно, q ложно влечет q истинно, если q не имеет значения истинности, то q истинно. Если Лжец - антиномия двузначной логики, то Усиленный Лжец - антиномия трехзначной, и для ее "решения" нужно ввести четвертое значение истинности, например, "неразрешимость q неразрешима". Но это тоже не предел... (Идея многозначных антиномий легко усматривается также в антиномии Помешанный Артур из [3].)

В настоящей статье антиномии:

q : q ложно или q неразрешимо,

r : r ложно или r неразрешимо или неразрешимость r неразрешима,

s : и т.д.

используются для построения "более чем неразрешимых" формул теории-объекта. Пусть T -теория, Q -ее метатеория. Неразрешимая формула Геделя как бы утверждает "я невыводима в T". Еще более неразрешимой будет формула, утверждающая,"в T выводимо мое отрицание или в Q доказуема моя неразрешимость".

2. А п п а р а т. Ради простоты изложения рассматриваются только рекурсивно аксиоматизированные теории первого порядка (с равенством) на языке формальной арифметики [4].

Теорию Q будем называть м е т а т е о р и е й теории T, если в Q выражено понятие о T-доказательстве. Более точно, во-первых, фиксировано рекурсивное $1-1$ -отображение формул и T-доказательств в натуральные числа (образы называются Q -и м е н а м и). Во-вторых, фиксированы формулы $Prf_T^{(Q)}(x,y)$, $Prf\ Neg_T^{(Q)}(x,y)$ со свободными x, y такие, что:

а) если n -имя T-доказательства формулы с именем m , то $\vdash_Q Prf_T^{(Q)}(\bar{m},\bar{n})$, в противном случае $\vdash_Q \neg Prf_T^{(Q)}(\bar{m},\bar{n})$.

б) если n -имя T -доказательства отрицания формулы с именем m то $\vdash_Q Prf\, Neg_T^{(Q)}(\bar{m},\bar{n})$, в противном случае $\vdash_Q \neg Prf\, Neg_T^{(Q)}(\bar{m},\bar{n})$.

Утверждение о том, что формула с Q -именем доказуема, опровержима или разрешима в T , можно выразить формулами:

$$Pr_T^{(Q)}(x) \rightleftharpoons (\exists y)\, Prf_T^{(Q)}(x,y),$$

$$Pr\, Neg_T^{(Q)}(x) \rightleftharpoons (\exists y)\, Prf\, Neg_T^{(Q)}(x,y),$$

$$Dec_T^{(Q)}(x) \rightleftharpoons (\exists y)[Prf_T^{(Q)}(x,y) \vee Prf\, Neg_T^{(Q)}(x,y)].$$

Теорию T будем называть ω^k -непротиворечивой $(0 \leqslant k < \omega)$, если для любой формулы $\mathfrak{A}$ следующие утверждения несовместимы

$$(a) \vdash_T \neg \mathfrak{A}(\bar{n}_1,\ldots,\bar{n}_k) \text{ для всех наборов } n_1 \ldots n_k$$

$$(б) \vdash_T (\exists x_1 \ldots \exists x_k)\, \mathfrak{A}(x_1 \ldots x_k).$$

При $k=0$ получается понятие (простой) непротиворечивости. Если в T выводимы все аксиомы формальной арифметики [4] , то при $k \geqslant 1$ ω^k-непротиворечивость равносильна ω -непротиворечивости. Наиболее естественным является, конечно, понятие $\exists$ -непротиворечивости (конъюнкция всех ω^k).

ЛЕММА 1. Пусть Q -метатеория теории T .
(1) Если m -имя формулы, разрешимой в T , то

$\vdash_Q Dec_T^{(Q)}(\overline{m})$.

(2) Если $\vdash_Q Dec_T^{(Q)}(\overline{m})$ и теория Q ω-непротиворечива, то формула с именем m разрешима в T.

(3) То же для формул Pr, $Pr\,Neg$.

Теорию T назовем **достаточно сильной**, если в ней **представима** любая общерекурсивная функция. Например, в случае 1-местной функции f для всех k, l:

$$f(k)=l \quad \text{влечет} \quad \vdash_T (\forall y)[F(\overline{k}, y) \equiv (y=\overline{l})].$$

В достаточно сильной теории **выразимо** любое рекурсивное отношение натуральных чисел, например:

$$A(k,l,m) \quad \text{влечет} \vdash_T \mathfrak{A}(\overline{k},\overline{l},\overline{m}),$$

$$\neg A(k,l,m) \quad \text{влечет} \vdash_T \neg\mathfrak{A}(\overline{k},\overline{l},\overline{m}).$$

Теория T будет достаточно сильной, если в ней выводимы все аксиомы теории Р.Робинсона [4].

ЛЕММА 2. Пусть формулы $F(x,y)$, $G(x,y)$ представляют в теории T функции f, g, причем $f(k)=l$, $g(l)=m$. Тогда для любой формулы $\mathfrak{A}$:

$$\vdash_T (\exists y)[F(\overline{k},y) \wedge \mathfrak{A}(y)] \equiv \mathfrak{A}(\overline{l}),$$

$$\vdash_T (\exists yz)[F(\overline{k},y) \wedge G(y,z) \wedge \mathfrak{A}(y,z)] \equiv \mathfrak{A}(\overline{l},\overline{m}).$$

3. **Теорема о двойной неполноте.** Пусть T -достаточно сильная теория, Q -ее метатеория. Тогда фиксирована формула $Dec_T^{(Q)}(x)$. С другой стороны, предполагая геделевскую арифметизацию T и Q, найдутся формулы $Prf_T^{(T)}(x,y)$, $Prf\,Neg_T^{(T)}(x,y)$, $Prf_Q^{(T)}(x,y)$, $Prf\,Neg_Q^{(T)}(x,y)$, выражающие в теории T понятия о T- и Q-доказательствах. Найдутся также:

(а) формула $Sub^{(T)}(x,y,z)$, представляющая в T функцию $z(x,y)$: "z есть (геделев) номер формулы, полученной из формулы с номером x подстановкой цифры $\bar{y}$ вместо всех свободных переменных",

(б) формула $Sub_*^{(T)}(x,y,z)$, представляющая в функцию "z есть номер формулы, полученной из формулы с номером x подстановкой Q -имени формулы с номером y вместо всех свободных переменных".

"Более чем неразрешимую" формулу теории T мы получим, моделируя антиномию

q : q ложно или q неразрешимо

в виде формулы, утверждающей: "в T выводимо мсе отрицание или в Q доказуема моя неразрешимость".

Возьмем следующую формулу $A(x)$:

$$(\exists y z)[Sub_1^{(T)}(x,x,y) \wedge Sub_*^{(T)}(\bar{\mu},y,z) \wedge$$
$$\wedge (\exists u)(Prf\ Neg_T^{(T)}(y,u) \vee Prf\ Neg_Q^{(T)}(z,y))],$$

где μ -номер формулы $Dec_T^{(Q)}(x)$ со свободной переменной x . Пусть m -номер формулы $A(x)$. Рассмотрим $A(\bar{m})$. По лемме 2 $A(\bar{m})$ эквивалентна

$$(\exists u)[Prf\ Neg_T^{(T)}(\bar{n},u) \vee Prf\ Neg_Q^{(T)}(\bar{\bar{\pi}},u)], \qquad (*)$$

где n -номер $A(\bar{m})$, π -номер $Dec_T^{(Q)}(\bar{a})$, a - имя $A(\bar{m})$.

ТЕОРЕМА 1 (теорема о двойной неполноте). Пусть T - достаточно сильная теория, Q -ее метатеория. Q -имя (замкнутой) формулы $A(\bar{m})$ обозначим через a .

(1) Если T ω -непротиворечива и Q -(просто) непротиворечива, то $A(\bar{m})$ невыводима в T и $\neg Dec_T^{(Q)}(\bar{a})$ недоказуема в Q .

(2) Если T непротиворечива, то $\neg A(\bar{m})$ невыводима в T .

(3) Если T и Q ω -непротиворечивы, то $Dec_T^{(Q)}(a)$ недоказуема в Q :

ДОКАЗАТЕЛЬСТВО.

(а) Пусть $\vdash_T A(\overline{m})$. Если T , Q непротиворечивы, то не $\vdash_T \neg A(\overline{m})$ и по лемме 1, не $\vdash_Q \neg Dec_T^{(Q)}(\bar{a})$. Поэтому для всех натуральных чисел s :

$$\vdash_T \neg Prf\ Neg_T^{(T)}(\bar{n},\bar{s}) \wedge \neg Prf\ Neg_Q^{(T)}(\bar{\bar{n}},\bar{s}).$$

Вместе с (*) это дает ω -противоречие в теории T

(б) Пусть $\vdash_T \neg A(\overline{m})$. Тогда:

$$\vdash_T (\exists z)\ Prf\ Neg_T^{(T)}(\bar{n},z),$$

т.е. $\vdash_T A(\overline{m})$. Противоречие в теории T .

(в) Пусть $\vdash_Q \neg Dec_Q^{(T)}(\bar{a})$. Тогда:

$$\vdash_T (\exists z)\ Prf\ Neg_Q^{(T)}(\bar{\bar{n}},\bar{z})$$

т.е. $\vdash_T A(\overline{m})$. См. теперь пункт (а).

(г) Пусть $\vdash_Q Dec_T^{(Q)}(\bar{a})$. Тогда по лемме 1, если Q ω -непротиворечива, то $A(\overline{m})$ разрешима в T . См. теперь пункты (а, б).

Теорема 1 доказана.

4. <u>Выводы</u>.

Итак, если достаточно сильная теория T ω -непротиворечива и выбрана какая-либо непротиворечивая ее метатеория Q , то в T найдется неразрешимое предложение, неразрешимость которого нельзя доказать средствами Q .

Теорему Геделя о неполноте можно истолковать как общее опровержение следующего "закона исключенного третьего": в математике всякая определенная гипотеза будет в конечном счете либо доказана, либо опровергнута, опираясь на традиционные математические представления. В таком случае теорема о двойной неполноте показывает, что нет оснований и для "закона исключенного четвертого": всякая определенная гипотеза будет в конечном счете либо доказана, либо опровергнута, либо будет доказана ее неразрешимость.

К сожалению, этот вывод не является новым. Неразрешимость гипотезы H можно считать надежно установленной, если в ZFC удалось вывести импликацию

$$Con(ZF) \to Con(ZFC + H) \wedge Con(ZFC + \neg H).$$

Давно известно, что "существует недостижимый кардинал" не является такой гипотезой.

5. О б о б щ е н и е. Используя многозначные антиномии, приведенные в разделе 1, нетрудно доказать теорему о тройной и вообще любой n -кратной неполноте. Все эти теоремы, а также теорема об ω -кратной неполноте и многие вариации на эту тему, содержатся в теореме 2.

Перечислимо растущее дерево метатеорий, это пара $\Sigma = (\mathfrak{M}, \varphi)$ где

(а) машина $\mathfrak{M}$ перечисляет непустое множество конечных кортежей натуральных чисел, причем так, что кортеж $(n_0\ n_1 \ldots n_k)$ перечисляется только п о с л е кортежей Λ, (n_0), $(n_0\ n_1)$, ..., $(n_0\ n_1 \ldots n_{n-1})$. Кортежи будем называть вершинами. Будем говорить, что вершина $(n_0 \ldots n_k)$ непосредственно вырастает из $(n_0 \ldots n_{k-1})$,

(б) ч.р. функция φ соотносит с каждой вершиной Q перечисляемого дерева некоторую теорию вместе с фиксированным способом, делающим Q метатеорией для теории, соотнесенной с вершиной T , из которой Q непосредственно вырастает. Исключение составляет вершина Λ (пустой кортеж), ей φ соотносит теорию-объект. Обозначения вершин и соответствующих теорий не различаются.

Пусть Σ -перечислимо растущее дерево метатеорий над теорией-объектом Λ . С каждой формулой F теории Λ ассоциируется перечислимая система формул $\{Dec_{FT} \mid T \in \Sigma\}$ где $Dec_{F\Lambda} = F$ и если Q непосредственно вырастает из T , то Dec_{FQ} -стандартная формула, утверждающая, что формула Dec_{FT} разрешима в теории T .

ТЕОРЕМА 2. Пусть $\sum$ -перечислимо растущее дерево ω -непротиворечивых метатеорий с достаточно сильной ω^2 -непротиворечивой теорией-объектом Λ . Тогда найдется замкнутая формула F теории Λ такая, что для всех $T \in \sum$ формула Dec_{FT} неразрешима в T .

ДОКАЗАТЕЛЬСТВО. Строится формула F , которая утверждает "существует $T \in \sum$ такое, что в T доказуема формула $\neg Dec_{FT}$,где F -это я". Квантор существования играет здесь роль бесконечной дизъюнкции (ср. антиномии в разделе 1). Если дерево $\sum$ имеет только конечное число вершин, достаточно потребовать ω -непротиворечивость теории-объекта Λ . В случае бесконечного $\sum$ нужна ω^2 -непротиворечивость Λ . Если предположить ω^3 -непротиворечивость Λ , доказательство можно провести и без информации о конечности-бесконечности дерева $\sum$.

6. Нерешенные проблемы.

1. Теорему о двойной неполноте легко доказать в следующей немного усиленной форме. Пусть T -достаточно сильная теория, Q -ее метатеория, T и Q ω -непротиворечивы. Найдется замкнутая T -неразрешимая формула (с именем a), для которой в Q недоказуема формула $\neg Pr_T^{(Q)}(\bar{a})$. Это действительно усиление, поскольку Q -недоказуемость $\neg Pr_T^{(Q)}(\bar{a})$ влечет недоказуемость $\neg Dec_T^{(Q)}(\bar{a})$, а недоказуемость $Pr_T^{(Q)}(\bar{a})$, $Pr\ Neg_T^{(Q)}(\bar{a})$, $Dec_T^{(Q)}(\bar{a})$ тривиальна в силу леммы 1. Неизвестно, можно ли обеспечить здесь одновременно Q -невыводимость еще и формулы $\neg Pr\ Neg_T^{(Q)}(\bar{a})$?

П. Пусть теория T (на языке формальной арифметики) $\exists$ -непротиворечива и: (а) в T доказуемы все истинные равенства, не содержащие переменных, (б) в T опродержимы все ложные равенства такого рода. Следуя решению 10-ой проблемы Гильберта [5] , можно построить диофантово уравнение $P(x_1 \dots x_k) = 0$, не имеющее решений в натуральных числах и такое, что формула

$$F \rightleftharpoons (\forall x_1 \dots \forall x_k)\, P(x_1 \dots x_k) \neq 0$$

неразрешима средствами теории T .

Заметим, однако, что в данном случае теория $T + \neg F$ оказывается $\exists$ -противоречивой, тогда как $T + F$, по-видимому, $\exists$ -непротиворечива. Таким образом, альтернатива "F или $\neg F$" не совсем безразлична для теории T , хотя она и неразрешима средствами T .

Возможна ли (замкнутая) формула G такая, что теории $T + G$, $T + \neg G$ обе $\exists$ -непротиворечивы? (Определение $\exists$ -непротиворечивости см. в разделе 2).

Ш. Теорию T назовем безгранично делимой, если любую независимую ее аксиому можно заменить на две новые аксиомы, не нарушая независимость и не меняя область выводимых формул. Это определение легко уточняется в каждом конкретном случае. Например, в случае исчисления высказываний фиксируются правила вывода: *modus ponens* и правило подстановки. Тогда "проблема деления" рассматривается для любой конечной независимой системы аксиом. Является исчисление высказываний безгранично делимым? Возможна ли бесконечная независимая система аксиом для (классического) исчисления высказываний?

1У. Введем в язык формальной арифметики переменную X для множеств натуральных чисел, допуская атомарные формулы вида $t \in X$, где t -произвольный терм. Известно [6] , что для любого множества A , перечислимого с оракулом B , найдется формула $F(x, X)$ такая, что для всех n : $n \in A$ если и только если $F(\bar{n}, B)$ -истинная формула. Можно ли обобщить решение 10-ой проблемы Гильберта [5] таким образом, чтобы в качестве всегда получалась формула вида

$$(\exists x_1 \dots \exists x_k)\, G(x, X, x, \dots x_k),$$

где G не содержит кванторов?

У. В классической арифметике, спекулируя на схеме $A \to (\neg A \to B)$, из любого противоречия легко выводится $0=1$. Осуществим ли такой вывод чисто арифметическими средствами, т.е. не используя $A \to (\neg A \to B)$? Например, $0=1$ арифметически следует из $4=5$ или из $(\exists x)(x=x+1)$. Но следует ли $0=1$ арифметически из любого противоречия $A \wedge \neg A$? Более точно, речь идет о возможности "универсального противоречия" в арифметике, использующей вместо классической логики т.н. минимальную логику [7] (плюс еще, быть может, закон двойного отрицания $\neg\neg \to A$).

ЛИТЕРАТУРА

1. Линдон Р. Заметки по логике. М., 1968.
2. Мостовский А. Конструктивные множества и их приложения. М., 1973.
3. Wormell C. P. On the paradoxes of self-reference, "Mind", 1958, v.67, No 266, pp. 267-271.
4. Мендельсон Э. Введение в математическую логику. М., 1971.
5. Матиясевич Ю.В. Диофантовы множества.–УМН, 1972, т.27, № 5.
6. Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. М., 1972.
7. Гастев Ю. Минимальная логика.–Философская энциклопедия, т. 3. М., 1964.

БЫСТРЫЕ ВЫЧИСЛЕНИЯ НА ВЕРОЯТНОСТНЫХ МАШИНАХ ТЬЮРИНГА

Р.В.Фрейвалд

Рассматривается обыкновенная одноленточная машина Тьюринга (без входа) с одной головкой на ленте, дополненная датчиком случайных чисел, выдающим символы 0 и 1 с равными вероятностями $\frac{1}{2}$ по бернуллиевской схеме, т.е. независимо друг от друга. Такую машину ниже будем называть вероятностной машиной Тьюринга.

Будем говорить, что вероятностная машина Тьюринга $\mathfrak{M}$ распознает множество A с вероятностью, превосходящей p ($\frac{1}{2} \leqslant p < 1$) за время $t(x)$, если при работе $\mathfrak{M}$ на произвольном слове x с вероятностью строго большей чем p произойдет следующее событие: машина остановится за не более чем $t(x)$ тактов с результатом

$$C_A(x) = \begin{cases} 1 & \text{, если } x \in A \\ 0 & \text{, если } x \in \bar{A} \end{cases}$$

Будем говорить, что вероятностная машина Тьюринга $\mathfrak{M}$ распознает множество A с вероятностью $1-o(1)$ за время $t(x)$, если для любого $\varepsilon > 0$ существует такое n, что при работе $\mathfrak{M}$ на произвольном слове x, длина которого превосходит n, с вероятностью строго большей чем $1-\varepsilon$ произойдет следующее: машина остановится за не более чем $t(x)$ тактов с результатом $C_A(x)$.

Я.М.Барздинь в [1] в частности доказал, что для любой (детерминированной) машины Тьюринга $\mathfrak{M}$, распознающей симметрию слов в двоичном алфавите, существует такая константа $c>0$, что для всех n, кроме конечного числа, максимум по всем словам x длины n времени работы $\mathfrak{M}$ на x превосходит $c \cdot n^2$.

ТЕОРЕМА 1. (1) Для каждого $\varepsilon>0$ существует вероятностная машина Тьюринга, которая распознает симметрию слов в двоичном алфавите с вероятностью, превосходящей $1-\varepsilon$, за время $c \cdot |x| \cdot \log_2^2 |x|$, где $|x|$ - длина слова x, а $c>0$ - константа, не зависящая от x.

(2) Существует вероятностная машина Тьюринга, которая распознает симметрию слов в двоичном алфавите с вероятностью $1-o(1)$ за время $c \cdot |x| \cdot \log_2^2 |x| \cdot \log_2 \log_2 |x|$, где $|x|$ - длина слова x, а $c>0$ - константа, не зависящая от x.

Сопоставление теоремы Барздиня и теоремы 1 показывает, что использование простейшего датчика случайных чисел дает возможность значительно увеличить скорость вычислений, даже если требуется, чтобы верный результат был выдан с большой вероятностью. Это дает положительный ответ на один вопрос Б.А.Трахтенброта [2].

Доказательство теоремы 1 опирается на следующие две леммы..

ЛЕММА 1. Если

$$\begin{cases} N' \equiv N'' \pmod{p_1} \\ N' \equiv N'' \pmod{p_2} \\ \text{-----------} \\ N' \equiv N'' \pmod{p_k} \end{cases},$$

где все $p_1, p_2, \ldots, p_k$ - попарно различные простые числа, то

$$N' \equiv N'' \,(\mathrm{mod}\; p_1 \cdot p_2 \cdot \cdots \cdot p_k)$$

ЛЕММА 2. Пусть $N' \leqslant 2^n$, $N'' \leqslant 2^n$ и $N' \neq N''$. Тогда существуют такие константы $c_1 > 0$ и $c_2 > 0$, что среди первых n^2 натуральных чисел встречается не менее чем $\left(c_1 \cdot \frac{n^2}{\log_2 n} - c_2 \cdot \frac{n}{\log_2 n}\right)$ простых чисел, которые не делят $|N' - N''|$ без остатка.

ТЕОРЕМА 2. Если некоторая вероятностная машина Тьюринга распознает симметрию слов в двоичном алфавите с вероятностью, превосходящей некоторое $p > \frac{1}{2}$, за время $t(x)$, то существует такая константа $c > 0$, что для бесконечно многих слов x $t(x) > c \cdot |x| \cdot \log_2 |x|$.

Б.А.Трахтенброт [3] доказал, что если некоторое множество распознаваемо на детерминированной машине Тьюринга за время $o(|x| \cdot \log_2 |x|)$, то это множество распознаваемо на конечном автомате.

Пусть B_1 - множество всех слов вида $0^n 1 0^n$ $(n = 0, 1, 2, \ldots)$

ТЕОРЕМА 3. Существует вероятностная машина Тьюринга, которая распознает множество B_1 с вероятностью $1 - o(1)$ за время $c \cdot |x| \cdot \log_2 \log_2 |x|$, где $|x|$ - длина распознаваемого слова x, а $c > 0$ - константа, не зависящая от x.

ТЕОРЕМА 4. Если некоторая вероятностная машина Тьюринга распознает множество B_1 с вероятностью, превосходящей некоторое $p > \frac{1}{2}$, за время $t(x)$, то существует такая константа $c>0$, что для бесконечно многих слов x

$$t(x) > c\cdot|x|\cdot \log_2 \log_2 |x| .$$

Теоремы 3 и 4 показывают, что для вероятностных машин Тьюринга теорема Трахтенброта не имеет места.

Дж. Гилл [4] высказал следующее предположение: если f - рекурсивная функция, и она вычислима на вероятностной машине Тьюринга с вероятностью, превосходящей некоторое $p>\frac{1}{2}$ за время $t(x)$, то существует также детерминированная машина Тьюринга, которая вычисляет f с такой временной сигнализирующей $\tilde{t}(x)$, что при некоторой $c>0$ для бесконечно многих x $\tilde{t}(x) \leqslant c\cdot t(x)$.

Пусть B_2 - множество всех слов x в однобуквенном алфавите, для которых существуют такие натуральные u и v , что 1) $0 \leqslant v < u$, и 2) длина слова x равна

$$2^{2^{2^{2^{u}}}} + v.$$

ТЕОРЕМА 5. (1) Существует вероятностная машина Тьюринга, которая распознает множество B_2 с вероятностью $1-o(1)$ за время $c\cdot|x|\cdot\log_2\log_2|x|$, где $|x|$ - длина распознаваемого слова, а $c>0$ - константа, не зависящая от x .

(2) Для любой детерминированной машины Тьюринга, распознающей множество B_2 , существует такая константа $c>0$, что для всех слов x , кроме конечного числа, время работы машины на аргументе x не меньше, чем $c\cdot|x|\cdot\log_2|x|$.
Таким образом, теорема 5 опровергает предположение Дж. Гилла.

Эта заметка была включена в сборник позже других статей. Ограничения на объем текста не позволили представить доказательства теорем. Предполагается, что эти доказательства будут опубликованы в другом месте.

ЛИТЕРАТУРА

1. Бардинь Я.М. Сложность распознавания симметрии на машинах Тьюринга.- В кн.: Проблемы кибернетики , 1965, вып. 15.
2. Трахтенброт Б.А. Замечания о сложности вычислений на вероятностных машинах. - В кн.: Исследования по теории алгорифмов и математической логике. М., 1974.
3. Трахтенброт Б.А. Сложность алгоритмов и вычислений. Новосибирск, 1967.
4. Gill J.T. III Computational complexity of probabilistic Turing machines. - Proc. 6-th Annual symposium ACM on theory of computing. 1974.

ABSTRACTS

Identifiability in the limit of the numbers of general recursive functions in various computable numberings

R.Freivalds

It is proved that there exists a computable numbering of all one - argument partial recursive functions such that if a class U of general recursive functions is identifiable in the limit, then U is finite. The reasons making a numbering complicated for the identification are investigated.

The relation between predictability and identifiability in the limit

R.Freivalds and J.Barzdin

It is proved that there exists a nonpredictable class of general recursive functions which is identifiable in the limit uniformly on all sequences of natural numbers. The uniform predictability on all sequences of natural numbers is equivalent to an identifiability in the limit when all the hypotheses are numbers of general recursive functions.

Comparing various concepts of function prediction and program synthesis. II

K.Podnieks

Prediction: $\varphi(m+1)$ is guessed from given $\varphi(0)\dots\varphi(m)$. Program synthesis: the program computing φ is guessed from given $\varphi(0) \dots \varphi(m)$. Maybe, the hypotheses H_m are correct for all sufficiently large m or with frequency ε . These approaches yield a hierarchy of prediction and program synthesis concepts. The comparison problem of any two concepts is solved.

On comparison of limit identification and standartization of general recursive functions

E. Kinber

Concepts of limit identification and standartization of functions are compared. It is proved, in particular, that there exists a limit standartizable class of recursive functions which is not identifiable in the limit.

Probabilistic prediction of function values

K.Podnieks

The value $\varphi(m+1)$ is guessed from given $\varphi(0)\ldots\varphi(m)$. Let $\tau(n,x)$ be a recursive function, set $\tau_n = \lambda x\,\tau(n,x)$. There is a probabilistic strategy R_τ , which makes $\lesssim \frac{1}{2}\log_2 n$ false predictions in the case τ_n with probability $\to 1$ as $n \to \infty$. This estimate is the best possible. Deterministic strategies do the same with the estimate $\simeq \log_2 n$.

Identification of automata by simple experiment when no upper bound on the number of states is given

J.Barzdin

It is proved that there exists a simple experiment which identifies automata with any preassigned frequency. An upper estimate of the length of such an experiment is obtained. This estimate is almost the best possible.

Construction of complete sample systems for programs with direct access method

J.Barzdin, A.Kalnins

A sample system is said to be complete for the given program, if every branch realizable by some arbitrary sample is realized by some sample in this system. The problem of construction of complete sample systems for correctness testing in the case of sequential access method was investigated in previous papers by the authors. In this paper the problem of construction of complete sample systems is investigated in the case of direct access method. Sufficient conditions for algorithmical solvability of this problem are obtained.

On complexity and optimality of the computation in the limit

R.Freivalds

Various measures of complexity for the computation in the limit are investigated. The optimality for infinitely many values of the argument and the optimality for almost all values of the argument are compared.

On frequecy real-time computations

E.Kinber

A concept of frequency computation of functions is considered. It is proved that there exist arbitrary complex functions which are frequency real-time computable.

Universal Buchberger automata and real-time computations

M.Auguston

The concept of Buchberger automaton generalizes many known formalisms of algorithm, such as Turing machine, Post machine, Markov normal algorithm.

A concept of real-time simulation on Buchberger automata is introduced. It is proved that there exists no universal general recursive Buchberger automaton simulating the class of general recursive automata in real time. A similar assertion is true for primitive recursive Buchberger automata.

The double-incompleteness theorem

K.Podnieks

Let T be a theory, Q - a metatheory of T. Under certain conditions there exist T - undecidable sentences for which this undecidability can not be proved in Q.

Fast computation by probabilistic Turing machines

R.Freivalds

It is shown that there exists a probabilistic Turing machine recognizing palindromes with probability $1-\varepsilon$ $(0<\varepsilon<\frac{1}{2})$ in $n\cdot(\log_2 n)^2$ time. For every probabilistic Turing machine recognizing palindromes with probability $1-\varepsilon$ $(0<\varepsilon<\frac{1}{2})$ the recognition time is proved to be $> const\cdot n\cdot \log_2 n$. A conjecture of J.T.Gill on restrictions of speed-ups by probabilistic machines is disproved.

СОДЕРЖАНИЕ

Ученые записки, том 233

ТЕОРИЯ АЛГОРИТМОВ И ПРОГРАММ

Выпуск II

Редакторы Э.Икауниекс, Т.Фадеева.
Технический редактор А.Анджан
Корректор А.Анджан

Латвийский государственный университет
Рига 1975

Подписано к печати IO.XI.1975. ЯТ 04291. Зак.№ 1344.
Ф/б 60x84/I6. Бумага №I. Физ.п.л.I3,5. Уч.-и.л.I0,3
Тираж 500 экз. Цена I р. 3 к.

Отпечатано на ротапринте, Рига-50, ул.Вейденбаума,5
Латвийский государственный университет им. П.Стучки

Цена I р. 3 к.

Учен. зап. (ЛГУ им. П.Стучки), 1975, т.233, I-210