Г. А. НАЗАРЯН

О РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ В АЛГОРИФМИЧЕСКИХ ЯЗЫКАХ

В настоящей работе рассматриваются оценки сложности реализации булевых функций в алгорифмических языках различных типов. При этом исследуются оценки сложности булевых функций, принадлежащих тем или иным классам функций, и основное внимание уделяется тому, для каких классов булевых функций и для каких алгорифмических языков возможны наилучшие (в асимптотическом смысле) оценки сложности реализации, определяемые из мощностных соображений. Таким образом, постановка вопроса сходна с аналогичными постановками в работах [13] и [6]. Однако специфика алгорифмических языков требует привлечения иных методов по сравнению с указанными работами. В п. 1 § 1 вводятся основные определения, используемые в статье, в частности, определяется понятие φ-равномерного относительно некоторого класса языков алгорифмического языка, играющее основную роль в дальнейшем; в принципе, алгорифмический язык называется φ-равномерным относительно некоторого класса языков, если для него совпадают асимптотические верхняя и нижняя оценки удлинения сообщений при трансляции из всевозможных языков рассматриваемого класса. (Понятие равномерного алгорифмического языка, таким образом, является обобщением понятия асимптотически оптимального языка [10]).

В п. 2 § 1 доказывается основная теорема о реализации булевых функций в алгорифмических языках, равномерных относительно класса языков. Согласно этой теореме оптимальные („мощностные“) оценки реализации булевых функций в алгорифмическом языке, равномерном относительно класса Π языков, имеют место для всякого конструктивного множества M булевых функций, такого, что его частичная характеристическая функция выражена в одном из языков класса Π, и количество n-местных функций из M или остается ограниченным, или стремится к бесконечности при возрастании n. В п. 3 § 1 устанавливаются также оценки изменения сложности реализации булевых функций при переходе от одной меры сложности к другой.

В § 2 п.п. 1, 2 доказывается, что условия основной теоремы выполняются для языка машин Тьюринга и языка нормальных алгорифмов (в фиксированных алфавитах); аналогичные факты устанавливаются также для алгорифмических языков (п. 3 § 3), основанных на рассмотрении классификации А. Гжегорчика [15].

Некоторые утверждения настоящей статьи в менее общем виде были изложены в докладе автора на конференции по алгорифмической теории сложности в г. Дилижане в мае 1971 г.

В заключение пользуюсь случаем выразить глубокую благодарность И. Д. Заславскому, под руководством которого выполнена настоящая работа.

§ 1

1°. Будем рассматривать слова в алфавите $\{0, 1\}$. Длину слова P обозначим через $l(P)$. Натуральные числа также определим как произвольные слова в алфавите $\{0, 1\}$, при этом роль нуля играет пустое слово, а роль операции следования алгорифм F такой, что для любого слова P в $\{0, 1\}$, $F(\Lambda) = 0$, $F(P0) = P1$, $F(P1) = F(P)0$ ([7], [10]). Для конкретных натуральных чисел сохраним обычные обозначения 0, 1, 2, ... ,. В работе приняты следующие сокращения: ч. р. ф. — „частично рекурсивная фракция“, б. ф. — „булева функция“, н. а. — „нормальный алгорифм“, м. т. — „машина Тьюринга“, р. п. м. — „рекурсивно перечислимое множество“. В дальнейшем буквы n, m, k, i, b, d (может быть с индексами) будут употребляться в роли переменных, допустимыми значениями которых являются любые натуральные числа, буква ε — любые положительные рациональные числа, буква г — любые FR-числа [11], буквы φ, ν, β — конструктивные функции ([8], [11]) типа (н → д), γ — конструктивные функции типа (д → д).

Мы будем основываться на конструктивном понимании суждений и на аппарате логико-математических языков из [12].

Приведем некоторые необходимые определения из [10]. Пусть A_j и A_i — алфавиты; $\square \overline{\in} A_i \cup A_j$; Ω — рекурсивное множество слов в A_i; U — н. а. над $A_i \cup A_j$ такой, что для всякого слова P в A_j и слова X, принадлежащего Ω, если $!\, U(X \square P)$, то $U(X \square P)$ есть слово в A_j. Список

$$Я = \langle A_j,\ A_i,\ \Omega,\ U \rangle \tag{1.1.1}$$

удовлетворяющий приведенным выше условиям, будем называть алгорифмическим языком, а всякое слово, принадлежащее Ω, сообщением этого языка. Мы будем рассматривать лишь такие языки, в которых множество Ω бесконечно; это условие в дальнейшем всюду подразумевается, если не оговорено противное.

Пусть $Я_1 = \langle A_{j_1}, A_{i_1}, \Omega_1, U_1 \rangle$ и $Я_1 = \langle A_{j_2}, A_{i_2}, \Omega_2, U_2 \rangle$ — два алгорифмических языка и пусть н. а. Θ над $A_{j_1} \cup A_{j_2}$ по каждому слову P в алфавите A_{j_1} выдает слово $\Theta(P)$ в алфавите A_{j_2}, имеющее при лексикографической нумерации слов в алфавите A_{j_2} ([7], п. 11:1) тот же номер, что и P при лексикографической нумерации слов в A_{j_1}. Будем называть н. а. T над $A_{l_1} \cup A_{l_2} \cup \{\square\}$ транслятором из $Я_1$ в $Я_2$, если он применим ко всякому сообщению X алгорифмического языка $Я_1$, причем $T(X) \in \Omega_2$ и для всякого слова P в A_j,

$$\Theta(U_1(X \square P)) \simeq U_2(T(X) \square \Theta(P)). \tag{1.1.2}$$

Перенумеруем все сообщения алгорифмического языка $Я = \langle A_j, A_l, \Omega, U \rangle$ в порядке возрастания их длин (сообщения с одинаковыми длинами упорядочим, например, лексикографически). Построим н. а. S над $A_l \cup \{0, 1\}$, перерабатывающий каждое сообщение языка $Я$ в его номер. Сообщение X с номером n $(S(X) = n)$ будем обозначать через X_n. Н. а. D над $A_l \cup \{0, 1\}$ будем называть мерой сложности [16] языка $Я$, если выполнены следующие условия:

1. Для любого сообщения X языка $Я$ $D(X)$ есть натуральное число.

2. Существует н. а. $\overline{D}$ над $A_l \cup \{0, 1, \square\}$ такой, что для любого натурального числа m $\overline{D}(m) = X_{m_1} \square \cdots \square X_{m_k}$, где для любого X_{m_l} $D(X_{m_l}) = m$ и для любого X такого, что $D(X) = m$ найдется i такое, что $X = X_{m_l}$ (здесь знак $=$ означает графическое равенство). Построим н. а. L над $\{0, 1\}$ такой, что для каждого сообщения X_i языка $Я$ выполнено $L(X_i) = l(i)$. Построенный н. а. L будем называть стандартной мерой сложности. Отметим, что в [10] н. а. с указанными свойствами именуется критерием сложности.

Нетрудно убедиться, что стандартная мера сложности есть мера сложности.

Сообщения X_n и X_m языка $Я = \langle A_j, A_l, \Omega, U \rangle$ будем называть эквивалентными, если для всякого слова P в A_j имеет место

$$U(X_n \square P) \simeq U(X_m \square P).$$

Пусть α и β какие-либо псевдофункции ([1], [2]), определенные для натуральных чисел и принимающие в качестве значений FR-числа. Через $\alpha(n) \underset{n}{\rightarrow} \infty$ будем обозначать суждение $\forall m \exists k \forall n (n > k \supset \alpha(n) > m)$. Через $\alpha(n) \underset{n}{\sim} \beta(n)$ будем обозначать суждение

$$\forall \varepsilon \exists d \forall n (n > d \supset |\alpha(n) - \beta(n)| < \varepsilon \cdot \beta(n).$$

Через $\alpha(n) \underset{n}{\lesssim} \beta(n)$ будем обозначать суждение

$$\forall \varepsilon \exists d \forall n (n > d \supset \alpha(n) \leqslant (1 + \varepsilon) \cdot \beta(n))$$

Запись $\alpha(n) \underset{n}{\gtrsim} \beta(n)$ означает $\beta(n) \underset{n}{\lesssim} \alpha(n)$. Запись $\alpha(n) \underset{n}{\eqsim} \beta(n)$ будет означать: для любой конструктивной строго возрастающей последовательности n_i натуральных чисел выполнено:

1) $\beta(n_i) \underset{i}{\to} \infty \supset \alpha(n_i) \lesssim \beta(n_i)$;

2) $\exists C_1 \forall i (\beta(n_i) < C_1) \supset \exists C \forall i (\alpha(n_i) < C)$.

Ясно, что $\alpha(n) \underset{n}{\lesssim} \beta(n)$ влечет $\alpha(n) \underset{n}{\lesseqqgtr} \beta(n)$, но обратное, вообще говоря, неверно.

Запись $\alpha(n) \underset{n}{\eqsim} \beta(n)$ будет означать $\beta(n) \underset{n}{\lesseqqgtr} \alpha(n)$ и $\alpha(n) \underset{n}{\cong} \beta(n)$ будет означать $\alpha(n) \underset{n}{\eqsim} \beta(n)$ и $\alpha(n) \underset{n}{\lesseqqgtr} \beta(n)$. Индекс n в записях $\alpha(n) \underset{n}{\sim} \beta(n)$, $\alpha(n) \underset{n}{\lesssim} \beta(n)$ и т. п. в дальнейшем будет иногда опускаться.

Замечание. Если в определении символа $\lesseqqgtr$ вместо конструктивной строго возрастающей последовательности натуральных чисел говорить о любых классических последовательностях (строго возрастающих), то хотя смысл определения изменился бы, однако все дальнейшие теоремы в рамках классической математики остались бы верными.

Пусть $Я$ — алгорифмический язык.

Через $\Phi^Я$ обозначим псевдофункцию, такую, что для любого FR-числа г, $\Phi^Я$(г) есть слово вида $X_0 \square X_1 \square \cdots \square X_n$, где n удовлетворяет условиям $L(X_n) \leqslant$ г и $L(X_{n+1}) >$ г. $\Phi^Я$(г) будем называть начальным г-фрагментом языка. Введем одноместную псевдофункцию $\lambda_Я$, такую, что для всякого FR-числа г значением этой псевдофункции является количество попарно неэквивалентных сообщений из $\Phi^Я$(г). Говорим, что φ есть миноранта для $Я$, если выполнено:

$$\forall \varepsilon \exists d \forall b (b > d \supset l(\lambda_Я((1-\varepsilon)\cdot\varphi(b))) < b). \quad (1.1.3)$$

Говорим, что φ есть функция плотности для языка $Я$, если:

1. φ — миноранта;

2. для всякой миноранты ν для $Я$ оказывается $\nu \lesssim \varphi$. Пусть L_1 и L_2 — стандартные меры сложности языков $Я_1$ и $Я_2$ соответственно. Пусть φ — конструктивная функция типа (н $\to$ д). Говорим, что $Я_1$ φ — сводится к $Я_2$, если существует транслятор T из $Я_1$ в $Я_2$, такой, что для любого ε можно построить d такое, что для любого сообщения X языка $Я_1$ выполнено

$$\forall b ((b > d) \supset (L_1(X) \leqslant b \supset L_2(T(X) \leqslant (1+\varepsilon)\cdot\varphi(b)).$$

Замечание 1.1.2. Нетрудно убедиться, что если φ — неубывающая неограниченная функция, то это определение эквивалентно следующему. Говорим, что $Я_1$ φ—сводится к $Я_2$, если существует транслятор T из $Я_1$ в $Я_2$, такой, что для любого ε можно построить d такое, что для любого сообщения X из $Я_1$ имеет место

$$L_1(X) > d \supset L_2(T(X)) \leqslant (1+\varepsilon)\cdot\varphi(L_1(X)).$$

Будем говорить, что язык $Я$ φ-оптимален относительно класса G алгорифмических языков, если любой язык из G φ-сводится к $Я$.

Язык $Я$ будем называть φ-оптимальным, если он φ-оптимален относительно класса всех алгорифмических языков.

Будем говорить, что $Я$ φ-равномерен относительно класса G алгорифмических языков, если:

1) $Я$ φ-оптимален относительно G;

2) φ есть функция плотности для языка $Я$.

Язык $Я$ будем называть φ-равномерным, если он φ-равномерен относительно класса всех алгорифмических языков.

Пусть φ^* — конструктивная функция типа (н → д), связанная с φ соотношением: для любого натурального n

$$\varphi^*(n) = \max_{i<n} \varphi(i).$$

Лемма 1.1.1. *Если φ есть миноранта для языка $Я$, то и φ^* также есть миноранта для языка $Я$.*

Доказательство. Так как φ миноранта, то для нее выполнено (1.1.3). Зафиксируем некоторое ε.

Пусть d таково, что

$$\forall b\,(b > d \supset l(\lambda_Я((1-\varepsilon)\cdot\varphi(b))) < b) \qquad (1.1.5)$$

Рассмотрим $\varphi^*(d)$. Очевидно, найдется d^*, такое, что $d^* > d$ и выполнено

$$\forall b\,(b > d^* \supset l(\lambda_Я((1-\varepsilon)\,\varphi^*(d))) < b). \qquad (1.1.6)$$

Из (1.1.5) имеем

$$\forall b\,(b > d \supset l(\lambda_Я((1-\varepsilon)\max_{d<i<b}\varphi(i))) < b). \qquad (1.1.7)$$

Учитывая монотонность функций l, $\lambda_Я$ и φ^*, из (1.1.6) и (1.1.7) имеем

$$\forall b\,(b > d^* \supset l(\lambda_Я((1-\varepsilon)\cdot\varphi^*(b))) < b).$$

Лемма доказана.

Говорим, что φ асимптотически монотонна, если $\varphi(n) \sim \max_{i<n}\varphi(i)$.

Лемма 1.1.2. *Если φ—функция плотности некоторого языка $Я$, то она асимптотически монотонна.*

Доказательство. Как и прежде, пусть $\varphi^*(n) \leqq \max_{i<n}\varphi(i)$. (Символ $\geqq$ будет обозначать „равенство по определению"). Нужно убедиться в том, что $\varphi(n) \sim \varphi^*(n)$ или что $\varphi \gtrsim \varphi^* \,\&\, \varphi \lesssim \varphi^*$. Соотношение $\varphi(n) \lesssim \varphi^*(n)$ очевидно. Соотношение $\varphi(n) \gtrsim \varphi^*(n)$ следует из леммы 1.1.1. В самом деле. Согласно лемме 1.1.1 φ^* есть миноранта, если φ миноранта и по пункту 2 определения функции плотности для любой миноранты, в частности, для φ^* будет $\varphi \gtrsim \varphi^*$.

Следствие. *Если алгорифмический язык $Я$ φ-равномерен относительно некоторого класса Π алгорифмических языков, то φ асимптотически монотонна.*

Будем говорить, что язык $Я$ является однозначным, если все сообщения языка попарно неэквивалентны.

Лемма 1.1.3. *Если φ — миноранта для $Я$, и к языку $Я$ φ-сводится некоторый однозначный язык $Я_1$, то φ есть функция плотности для $Я$.*

Доказательство. Достаточно убедиться, что выполнено второе условие определения функции плотности, т. е. для всякой миноранты ν языка $Я$ оказывается $\nu \lesssim \varphi$.

Пусть ν—миноранта. Зафиксируем некоторое ε. Подберем ε_1 и ε_2 так, чтобы выполнялось

$$(1+\varepsilon_2) < (1-\varepsilon_1)\cdot(1+\varepsilon). \tag{1.1.8}$$

Используя второе определение φ сводимости языка $Я_1$ к $Я_2$ (см. замечание 1.1.2) и то, что $Я_1$ однозначен, нетрудно убедиться, что для некоторого d_2 выполнено соотношение

$$\forall b\,(b > d_2 \supset l\,(\lambda_Я\,((1+\varepsilon_2)\cdot\varphi\,(b))) \geqslant b) \tag{1.1.9}$$

В силу монотонности $\lambda_Я$ из (1.1.8) и (1.1.9) для $b > d_2$ имеем

$$l\,(\lambda_Я\,((1-\varepsilon_1)\cdot(1+\varepsilon)\cdot\varphi\,(b))) > b. \tag{1.1.10}$$

С другой стороны, т. к. ν миноранта, то для некоторого d_1 выполнено

$$\forall b\,(b > d_1 \supset l\,(\lambda_Я\,(1-\varepsilon_1)\cdot\nu\,(b))) < b). \tag{1.1.11}$$

Из (1.1.10) и (1.1.11) для $d=\max\{d_1, d_2\}$ в силу монотонности $\lambda_Я$ выполнено: если $b > d$, то

$$(1-\varepsilon_1)\cdot\nu\,(b) \leqslant (1-\varepsilon_1)\cdot(1+\varepsilon)\cdot\varphi\,(b),$$

или

$$\nu\,(b) \leqslant (1+\varepsilon)\,\varphi\,(b).$$

Таким образом, окончательно имеем

$$\forall\varepsilon\,\exists d\,\forall b\,(b > d \supset \nu\,(b) < (1+\varepsilon)\cdot\varphi\,(b)).$$

или $\nu\,(b) \lesssim \varphi\,(b)$, что и требовалось доказать.

2°. Натуральное число f длины 2^n ($n=0, 1, 2, \ldots$) будем называть булевой функцией от n переменных. Через $\sigma\,(i, p)$ обозначим ч. р. ф., такую, что при любых i и p

$$\sigma\,(i, p) = \mathrm{rest}\,([\,p+1-2^{l(p)}/2^{l(p)-i}\,], 2)$$

(здесь rest определяется так же, как в [7]).
Легко видеть, что при $1 \leqslant i \leqslant l\,(p)$ значение $\sigma\,(i, p)$ равно 0, если i-тая буква, начиная слева, слова p (при нумерации букв в слове, начинающейся с единицы) есть **0**, и $\sigma\,(i, p)=1$, если i-тая буква слова p есть **1**.

Через ν обозначим алгорифмическую функцию, такую, что

$$\nu(x) = \sum_{k=1}^{l(x)} \sigma(k, x) 2^{l(x)-k}.$$

Легко видеть, что $\nu(x)$ есть натуральное число, запись которого в двоичной системе счисления получится исходя из x посредством замены **0** на 0 и **1** на 1.

Значением б. ф. f от n переменных на натуральном числе x длины n будем называть число $\sigma(\nu(x), f)$, которое будем обозначать через $f(x)$.

Пусть $Я \gtrapprox \langle A_j, A_l, \Omega, U \rangle$ — алгорифмический язык и $A_j \supset \{\mathbf{0}, \mathbf{1}\}$. Говорим, что сообщение X языка $Я$ реализует б. ф. f от n аргументов (кратко будем записывать $X \rightrightarrows f$), если для любого слова P в $\{\mathbf{0}, \mathbf{1}\}$ длины n имеет место $U(X \square P) = f(P)$. Пусть M — рекурсивно перечислимое множество б. ф. Через M_n будем обозначать множество б. ф. от n переменных, принадлежащих M. Для каждого конструктивного множества M б. ф. введем одноместную псевдофункцию d_M, такую, что для всякого n значением $d_M(n)$ этой псевдофункции является количество б. ф., принадлежащих M.

Пусть в языке $Я$ для всякой б. ф. f можно построить сообщение X, такое, что $X \rightrightarrows f$. Пусть D — мера сложности языка $Я$. Говорим, что сообщение X является D-минимальным для б. ф. f, если X реализует f, и для любого сообщения X' языка $Я$ такого, что X' реализует f, выполнено $D(X') \geqslant D(X)$. Через $DM_n^Я$ будем обозначать конструктивное множество сообщений из $Я$, такое, что сообщение X языка $Я$ принадлежит $DM_n^Я$, тогда и только тогда, когда оно D-минимально для некоторой б. ф. из M_n. Одноместную псевдофункцию $D_M^Я$ определим следующим образом:

$$D_M^Я(n) = \begin{cases} 0, & \text{если } M_n \text{ пусто;} \\ \max\limits_{X \in DM_n^Я} D(X), & \text{если } M_n \text{ непусто} \end{cases}$$

Стандартная мера сложности L есть частный случай меры сложности. Мы будем употреблять обозначения $LM_n^Я$ и $L_M^Я$, которые будут пониматься в соответствии с определением $DM_n^Я$ и $D_M^Я$.

Если какая-либо буква R обозначает некоторый класс ч. р. ф., то R-множествами будем называть такие рекурсивные множества, характеристические функции которых принадлежат R.

Пусть $П$ — класс ч. р. ф. и β — конструктивная функция типа (н → д). Говорим, что язык $Я$ является β-мощностным для П-множеств б. ф. по мере сложности $D^Я$, если для любого П-множества M б. ф. выполнено $D_M^Я(n) \cong \beta(l(d_M(n)))$.

Произвольную двухместную ч. р. ф. будем называть нумерацией. С каждой нумерацией ψ естественным образом ассоциируется алгорифмический язык $Я_\psi$.

$$Я_\varphi = \langle \{0, 1\}, \{0, 1\}, N, \bar{\varphi} \rangle \qquad (1.2.1)$$

сообщения которого суть натуральные числа, N — множество натуральных чисел и $\bar{\varphi}$ есть н. а. над $\{0, 1\}$, такой, что для любых натуральных чисел p и x

$$\bar{\varphi}(p \square x) \simeq \varphi(p, x). \qquad (1.2.2)$$

Отметим, что стандартной мерой сложности языка $Я_\varphi$ является н. а. L над $\{0, 1\}$, применимый к любому натуральному числу p и такой, что $L(p) = l(p)$.

Пусть $П$ — класс ч. р. ф. и $П_2$ — класс нумераций из $П$. Через $\overline{П}_2$ будем обозначать класс языков нумераций из $П_2$. Через E^k будем обозначать k-тый ($k = 0, 1, \ldots$) класс функций в иерархии А. Гжегорчика [15].

Теорема 1.2.1. *Пусть класс частично рекурсивных функций $П$ содержит E^3 и замкнут относительно суперпозиции и операции ограниченного минимума. Пусть язык $Я$ φ-оптимален относительно $\overline{П}_2$. Тогда*

$$L_M^Я(n) \approxeq \varphi(l(d_M(n)))$$

для любого $П$-множества M б. ф.

Доказательство. Пусть θ — н. а., определяющий взаимнооднозначное соответствие между словами в $\{0, 1\}$ и словами в алфавите $A_j = \{a_0, a_1, \ldots, a_k\}$ (где $k \geqslant 2$ и $a_0 = 0$, $a_1 = 1$) такое, как указано на стр. 37. Так как M есть $П$-множество, то характеристическая функция δ множества M принадлежит $П$. Но класс $П$ содержит E^3 и замкнут относительно подстановки и ограниченного минимума, а потому функция

$$g(p, n) = \mu_{x < 2^{2^n}+1} x\, [\delta(x) = 0 \,\&\, l(x) = 2^n \,\&\, \forall_{0<i<p-1} i\,(x \neq g(i, n))]$$

принадлежит $П$. Нетрудно убедиться, что при всяком фиксированном n_0 функция $g(p, n_0)$ перечисляет M_{n_0} без повторений при $p < d_M(n)$. Используя функцию g, легко построить функцию ψ, принадлежащую классу $П$ и удовлетворяющую следующему условию: для любого натурального числа x, если $\theta(x)$ не есть натуральное число (т. е. не есть слово в алфавите $\{0, 1\}$), то $\psi(p, x) = 0$, если же $\theta(x)$ есть натуральное число, то

$$\psi(p, x) = \sigma(\nu(\theta(x)), g(p, l(\theta(x)))) + 1.$$

Будем говорить, что ψ разрешает б. ф. f от n аргументов при заданном p, если для любого натурального числа x, такого, что $\theta(x)$ есть натуральное число и $l(\theta(x)) = n$ выполнено

$$\psi(p, x) = \sigma(\nu(\theta(x)), f) + 1.$$

Как нетрудно убедиться, если $\lambda pg(p, n)$ перечисляет б. ф. из M, то ψ при тех же p разрешает б. ф. из M_n.

Пусть $Я_\psi$ — алгорифмический язык, ассоциированный с ψ (см. 1.2.1). Так как по предположению $Я_\psi$ принадлежит $\overline{\Pi}_2$, то существует транслятор T из $Я_\psi$ в $Я$, φ — сводящий $Я_\psi$ к $Я$. Из определения транслятора T имеем: для любых натуральных чисел p и x (напомним, что сообщения $Я_\psi$ суть натуральные числа) выполнено

$$\theta(\bar{\psi}(p \square x)) \simeq U(T(p) \square \theta(x)).$$

Для облегчения ссылок дальнейшие рассуждения разобьем на части, помеченные посредством a0, a1, a2, a4.

a0. Нетрудно убедиться, что если ψ разрешает б. ф. f от n переменных при p, то сообщение $T(p)$ языка $Я$ реализует б. ф. f. Функция $\lambda pg(p, n)$ перечисляет без повторений б. ф. из M_n при $p < d_M(n)$, и функция ψ при тех же p разрешает соответствующие булевы функции.

a1. Если ψ разрешает б. ф. f при p, то говорим, что сообщение p языка $Я_\psi$ разрешает б. ф. f. Таким образом, для любой б. ф. f из M найдется сообщение X языка $Я_\psi$, такое, что X разрешает б. ф. f и для стандартной меры сложности $L^{Я_\psi}$ языка $Я_\psi$ выполнено $L^{Я_\psi}(X) \leqslant l(d_M(n))$.

a2. Так как среди нумераций, принадлежащих Π_2, существуют однозначные (говорим, что нумерация $\pi(n, x)$ — однозначная, если из $n_1 \neq n_2$ следует $\urcorner(\pi(n_1, x) \simeq \pi(n_2, x))$), то, как нетрудно убедиться, $\varphi(n) \to \infty$, и если для конструктивной последовательности чисел n_i существует константа C_1, такая, что для всех i $\varphi(l(d_M(n_i))) < C_1$, то найдется константа C_2 такая, что для всех i $l(d_M(n_i)) < C_2$. Сообщения фрагмента $\Phi^{Я_\psi}(C_2)$ транслятором T транслируются в фрагмент $\Phi^{Я}(C_3)$, где C_3 — константа. Таким образом, из $\exists C_1 \forall_i (\varphi\, l(d_M(n_i))) < C_1)$ следует, что $\exists C_3 \forall_i (L^{Я}_{M}(n_i) < C_3)$.

a3. Пусть конструктивная последовательность чисел n_i такова, что $\varphi(l(d_M(n_i))) \underset{i}{\to} \infty$. Как нетрудно убедиться, из $\varphi(l(d_M(n_i))) \underset{i}{\to} \infty$ следует, что $l(d_M(n_i)) \underset{i}{\to} \infty$.

a4. Зафиксируем ε. Пусть d таково, что

$$\forall X \forall b\, ((b > d) \supset (L^{Я_\psi}(X) < b \supset L^{Я}(T(X)) \leqslant (1+\varepsilon) \cdot \varphi(b))). \quad (1.2.3)$$

Для случая $\varphi(l(d_M(n_i))) \to \infty$ имеем из a3, что $l(d_M(n_i)) \to \infty$ и, следовательно, найдется i_0 такое, что для всех $i > i_0$ выполнено $l(d_M(n_i)) > d$. В соответствии с a1 для любой б. ф. f из M_n найдется сообщение X языка $Я_\psi$, разрешающее f, и при этом транслированные сообщения $T(X)$ языка $Я$ реализуют f и (см. a0) $L^{Я_\psi}(X) \leqslant l(d_M(n))$.

Таким образом, с учетом (1.2.3) имеем

$$\forall_i ((i \geqslant i_0) \supset (L^{Я}_{М}(n_i) < (1+\varepsilon)\cdot\varphi(l(d_М(n_i))))),$$

и окончательно

$$L^{Я}_{М}(n_i) \underset{i}{\lesssim} \varphi(l(d_М(n_i))). \qquad (1.2.4)$$

Из (1.2.4) с учетом а2 имеем

$$L^{Я}_{М}(n) \eqsim \varphi(l(d_М(n))).$$

Теорема доказана.

В доказательстве теоремы использовались методы и результаты, установленные А. Н. Колмогоровым в [4] и [3] (см. [3] теорема 1.3).

Для класса Ч всех ч. р. ф. имеет место усиленная форма теоремы 1.2.1.

Теорема 1.21*. *Если язык Я φ-оптимален относительно Ч, то*

$$L^{Я}_{М}(n) \eqsim \varphi(l(d_М(n)))$$

для любого р. п. м. М б. ф.

Доказательство такое же, как и доказательство теоремы 1.2.1, с той лишь разницей, что построение функции g производится на основании теорем о перечислении р. п. м. посредством неповторяющихся ч. р. ф.

Лемма 1.2.1 *Если φ-миноранта для Я и в языке Я реализуются все функции из р. п. м. М, то*

$$L^{Я}_{М}(n) \eqsim \varphi(l(d_М(n))).$$

В соответствии с определением символа $\eqsim$ для строго возрастающей конструктивной последовательности натуральных чисел n_i рассмотрим случаи

$$L^{Я}_{М}(n_i) \underset{i}{\to} \infty \quad \text{и} \quad \forall_i (L^{Я}_{М}(n_i) < C).$$

Из $\forall i (L^{Я}_{М}(n_i) < C)$ следует, что $\forall i (l(d_М(n_i)) < C)$ и следовательно, $\forall i (\varphi(l(d_М(n_i))) < C_1)$. Пусть $L^{Я}_{М}(n_i) \to \infty$. Убедимся, что

$$L^{Я}_{М}(n_i \gtrsim \varphi(l(d_М(n_i))).$$

Зафиксируем некоторое ε.

По предположению φ есть миноранта, а потому можно построить d, удовлетворяющее условию

$$\forall b (b > d \supset l(\lambda_Я((1-\varepsilon)\cdot\varphi(b))) < b). \qquad (1.2.3)$$

Т. к. $L^{Я}_{М}(n_i) \to \infty$, то найдется i_0 такое, что

$$\forall i (i > i_0 \supset [L^{Я}_{М}(n_i) > \max_{b<d}((1-\varepsilon)\cdot\varphi(b))]). \qquad (1.2.4)$$

Для $i > i_0$ таких, что $l(d_M)(n_i)) > d$ из (1.2.3) имеем

$$l(\lambda_Я((1-\varepsilon)\cdot\varphi(l(d_M(n_i))))) < l(d_M(n_i)) \qquad (1.2.5)$$

Из определения L имеем $L_M^Я(n) \geqslant l(d_M(n))$.

Из определения $L_M^Я$ имеем

$$l(\lambda_Я(L_M^Я(n))) \geqslant l(d_M(n)). \qquad (1.2.6)$$

Из (1.2.5) и (1.2.6) в силу монотонности $\lambda_Я$ имеем: для любых $i \geqslant i_0$, таких, что $l(d_M(n_i)) \geqslant d$, выполнено

$$L_M^Я(n_i) \geqslant (1-\varepsilon)\cdot\varphi(l(d_M(n_i))). \qquad (1.2.7)$$

Для $i \geqslant i_0$, таких, что $l(d_M(n_i)) < d$ из (1.2.4) имеем

$$L_M^Я(n_i) \geqslant (1-\varepsilon)\cdot\varphi(l(d_M(n_i))). \qquad (1.2.8)$$

Из (1.2.8) и (1.2.7) имеем

$$\forall i((i \geqslant i_0) \supset [(L_M^Я(n_i) \geqslant (1-\varepsilon)\cdot\varphi(l(d_M(n_i)))])$$

и окончательно

$$L_M^Я(n_i) \gtrsim \varphi(l(d_M(n_i))).$$

Лемма доказана.

Теорема 1.2.2. *Пусть класс частично рекурсивных функций $П$ содержит E^3 и замкнут относительно суперпозиции и операции ограниченного минимума. Тогда если язык $Я$ φ-равномерен относительно $\overline{П}_2$, то $Я$ φ-мощностной для $П$-множеств б. ф. по мере сложности L.*

Доказательство. Нужно доказать, что $L_M^Я(n) \simeq \varphi(l(d_M(n)))$ для любого $П$-множества M. Это сразу следует из теоремы 1.2.1 и леммы 1.2.1.

Как нетрудно убедиться, асимптотически оптимальный язык φ-равномерен при $\varphi(x) = x$ и имеет место.

Следствие 1.2.1. *Для любого асимптотически оптимального $Я$ с критерием сложности L выполнено*

$$L_M^Я(n) \cong l(d_M(n)).$$

для любого рекурсивного перечислимого множества M.

В [10] дается определение мультипликативно оптимального языка. Нетрудно убедиться, что мультипликативно оптимальный язык с константой C есть φ-оптимальный алгорифмический язык при $\varphi(x) = C\cdot x$, и, как следует из теоремы 1.2.1.

Следствие 1.2.2. *Каков бы ни был мультипликативно оптимальный язык $Я$ с константой C, имеет место*

$$L_M^Я(n) \lesseqgtr C\cdot l(d_M(n))$$

для любого рекурсивно перечислимого множества M.

3°. Перейдем к нахождению оценок функций Шеннона для одной меры сложности, когда известны оценки для функций Шеннона для другой меры и эти меры связаны некоторой зависимостью.

Распространим определение асимптотической монотонности на конструктивные функции действительной переменной (типа (д → д)). Пусть γ — конструктивная функция типа (д → д) и γ^* — конструктивная функция типа (н → д), связанная с γ^* соотношением $\gamma^*(n) = \max\limits_{i<n} \gamma(i)$ (напомним, что i — переменная, допустимые значения которой суть натуральные числа). Говорим, что γ асимптотически монотонна, если $\gamma^* \sim \gamma$.

Лемма 1.3.1. *Если n_i^1 и n_i^2 — две псевдопоследовательности натуральных чисел, такие, что $n_i^1 \to \infty$ и $\forall i (n_i^1 \geqslant n_i^2)$ и γ асимптотически монотонна, то $\gamma(n_i^1) \underset{i}{\gtrsim} \gamma(n_i^2)$.*

Доказательство. Нужно убедиться, что выполнено

$$\forall \varepsilon \exists d \forall m \left(m > d \supset \frac{\gamma(n_m^1)}{\gamma(n_m^2)} > 1 - \varepsilon \right).$$

Так как γ асимптотически монотонна, то для всякого фиксированного ε имеем

$$\exists k \forall n \left(n > k \supset \frac{\gamma(n)}{\gamma^*(n)} > 1 - \varepsilon \right) \tag{1.3.1}$$

(Напомним, что $\gamma^*(n) = \max\limits_{i<n} \gamma(i)$).

Из $n_m^2 < n_m^1$ следует, что $\gamma(n_m^2) \leqslant \gamma^*(n_m^1)$. Следовательно, для любого n_i $(i = 0, 1, \ldots)$ имеем

$$\frac{\gamma(n_i^1)}{\gamma(n_i^2)} \geqslant \frac{\gamma(n_i^1)}{\gamma^*(n_i^1)}. \tag{1.3.2}$$

Т. к. $n_i^1 \to \infty$, то найдется d такое, что для всех $m > d$ выполнено $n_m > k$; из (1.3.1) имеем

$$\exists d \forall m \left(m > d \supset \frac{\gamma(n_m^1)}{\gamma^*(n_m^1)} > 1 - \varepsilon \right). \tag{1.3.3}$$

Из (1.3.2) и (1.3.3) имеем

$$\exists d \forall m \left(m > d \supset \frac{\gamma(n_m^1)}{\gamma(n_m^2)} > 1 - \varepsilon \right).$$

Лемма доказана.

Теорема 1.3.1. *Пусть $D^Я$ и $G^Я$ — меры сложности языка Я, связанные соотношением*

$$D^Я(X) \underset{G(X)\to\infty}{\sim} \gamma(G^Я(X)). \tag{1.3.4}$$

Тогда, если γ *асимптотически монотонна, то при* $d_M(n) \to \infty$ *будет*

$$D_M^Я(n) \sim \gamma(G_M^Я(n)).$$

для любого р. п. м. М.

Доказательство. По определению D_M

$$D_M(n) = \max_{X \in DM_n^Я} D(X) \sim \max_{X \in DM_n^Я} (\gamma(G(X)). \tag{1.3.5}$$

Построим псевдопоследовательность сообщений X_n такую, что начиная с некоторого n $X_n \in DM_n$ и

$$\max_{X \in DM_n^Я} G(X) = G(X_n). \tag{1.3.6}$$

Так как $X_n \in DM_n^Я$, то

$$\max_{X \in DM_n^Я} \gamma(G(X)) \geqslant \gamma(G(X_n)). \tag{1.3.7}$$

В силу выбора X_n имеем $G(X_n) \geqslant G_M^Я(n)$. Нетрудно убедиться, что из $d_M(n) \to \infty$ следует $G(X_n) \to \infty$ и по лемме 1.3.1

$$\gamma(G(X_n)) \gtrsim \gamma(G_M^Я(n)), \tag{1.3.8}$$

и окончательно имеем

$$D_M^Я(n) \gtrsim \gamma(G_M^Я(n)).$$

Докажем теперь обратное соотношение. Имеем

$$D_M^Я(n) \leqslant \max_{X \in MG_n^Я} D(X) \sim \max_{X \in GM_n^Я} \gamma(G(X)). \tag{1.3.9}$$

Пусть псевдопоследовательность сообщений X_n языка $Я$ такова, что начиная с некоторого n $X_n \in GM_n^Я$ и

$$\max_{X \in GM_n^Я} \gamma(G(X)) = \gamma(G(X_n)) \tag{1.3.10}$$

Так как $G(X_n) \leqslant G_M^Я(n)$ и $G_M^Я(n) \to \infty$, то по лемме 1.3.1

$$\gamma(G(X_n)) \lesssim \gamma(G_M^Я(n))$$

и

$$D_M^Я(n) \lesssim \gamma(G_M^Я(n)), \tag{1.3.11}$$

и окончательно

$$D_M^Я(n) \sim \gamma(G_M^Я(n)).$$

Теорема доказана.

Говорим, что функция γ асимптотически непрерывна, если для любых псевдофункций a и b типа (н $\to$ д) из $a(n) \to \infty$ и $a(n) \sim b(n)$ следует $\gamma(a(n)) \sim \gamma(b(n))$.

Суперпозицию функций γ и φ будем обозначать посредством $\gamma * \varphi$ (таким образом, $(\gamma * \varphi)(x) = \gamma(\varphi(x))$).

Пусть Π — некоторый класс ч. р. ф.

Теорема 1.3.2. *Пусть γ асимптотически монотонна и асимптотически непрерывна и меры сложности D и G связаны соотношением (1.3.4). Тогда, если язык $Я$ φ-мощностной для Π-множеств по мере сложности G, то $Я$ $\gamma * \varphi$-мощностной для Π-множеств по мере сложности D.*

Доказательство следует из теоремы 1.3.1.

Отметим еще следующую модификацию утверждений настоящего параграфа. Определим некоторый специальный вид сводимости языков, которую будем называть нумерической. Пусть $Я_1 = \langle A_{j_1}, A_{l_1}, \Omega_1, U_1 \rangle$ и $Я_2 = \langle A_{j_2}, A_{l_2}, \Omega_2, U_2 \rangle$ — алгоритмические языки. Не нарушая общности (предполагая, что мощности алфавитов A_{j_1} A_{j_2} не меньше двух), можем считать, что $A_{j_1} \supset \{0, 1\}$ и $A_{j_2} \supset \{0, 1\}$. Говорим, что сообщение X языка $Я$ изображает ч. р. ф. f, если для любого натурального числа n $U(X \square n) \simeq f(n)$. Говорим, что $Я_1$ нумерически сводится к $Я_2$ если существует транслятор T из $Я_1$ в $Я_2$, такой, что для любого сообщения X языка $Я_1$, изображающего некоторую ч. р. ф. оказывается: для всякого натурального числа P $U_1(X \square P) \simeq U_2(T(X) \square P)$. Тогда все утверждения настоящего параграфа (в частности теорема 1.2.1) верны также для того случая когда в основу определений положена нумерическая сводимость (отметим, что для случая нумерической сводимости доказательство теоремы 1.2.1 незначительно отличается от приведенного выше).

§ 2

В этом параграфе мы рассмотрим оценки функций Шеннона для мер сложности языков машин Тьюринга и нормальных алгоритмов. Для языка машин Тьюринга меру сложности определим как число внутренних состояний машин Тьюринга; для языка нормальных алгоритмов — как длину изображений нормальных алгоритмов.

1°. Пусть $A = \{a_0, \ldots, a_{k-1}\}$ некоторый фиксированный алфавит из k букв ($k \geqslant 3$), где $a_1 = 0$, $a_2 = 1$, a_0 рассматривается как символ пустого состояния ячейки на ленте м. т. Будем рассматривать м. т. с внешним алфавитом A. Все понятия, связанные с м. т. и здесь не определяемые, понимаются как в [7]. Состояния внутренней памяти будем обозначать символами $q_0, q_1, \ldots, q_{m-1}$. Команды м. т. имеют вид $q_i a_j \to q_k v_{ij}$, где $v_{ij} \in A \cup \{L, R\}$. Состояние q_0 — выделенное (заключительное). Для каждых q_i и a_j $i = 1, \ldots, m-1$, $a_j \in A$, программа машины содержит одну и только одну команду, начинающуюся словом $q_i a_j$. Программа м. т. содержит в точности $k \cdot (m-1)$ команд. Каждой м. т. Π поставим в соответствие шифр $\Pi^{ш}$ аналогично тому, как это сделано в [7]. Для шифров выполнено следующее условие: при фиксированном алфавите A чем больше внутренних состояний у м. т., тем длиннее ее шифр. Пусть e_1 и e_2 дополнительные буквы, необходимые для записи шифров. Рассмотрим алфавит $A' = \{L, R, e_1, e_2\} \cup A$. Множество шифров обозначим через Ω. Построим н. а. V над A' такой, что для любого слова P в A и любой м. т. Π с программой $\overline{\Pi}$ имеет место

$$V(\Pi^{\text{ш}} \square P) \simeq \overline{\Pi}(P). \tag{2.1.1}$$

Нетрудно убедиться, что таким образом определенная четверка $\langle A, A', \Omega, V \rangle$ является алгорифмическим языком. Этот язык будем называть языком машин Тьюринга. Натуральное число k, равное мощности алфавита A, будем называть параметром языка м. т.. Через $D(\Pi)$ и $D(\Pi^{\text{ш}})$ будем обозначать число внутренних состояний м. т., имеющей программу Π.

Теорема 2.1.1. *Всякий язык машин Тьюринга φ-равномерен, где* $\forall x\left(\varphi(x) = \frac{k}{k-1}x\right)$.

Доказательство. Вначале сформулируем два очевидных предложения.

1. Если универсальный алгорифмический язык $Я_1$ сводится к алгорифмическому языку $Я_2$, то $Я_2$ универсален.

2. Если $Я_1$ — аддитивно оптимальный язык [10] φ-сводится к $Я_2$ и φ есть многочлен с рациональными коэффициентами, то $Я_2$ φ — оптимален.

Как следует из предложений 1 и 2, для доказательства φ-оптимальности языка машин Тьюринга $\left(\varphi(x) = \frac{k}{k-1}x\right)$ достаточно φ-свести к нему какой-либо аддитивно оптимальный язык.

Если U — аддитивно оптимальная универсальная для класса всех одноместных ч. р. ф. функция (см. § 1.2), то ассоциированный с ней язык (см. (1.2.1))

$$Я_1 = \langle \{0, 1\}, \ \{0, 1\}, \ N, \ \tilde{U} \rangle$$

аддитивно оптимален. Убедимся, что $Я_1$ φ-сводится, где $\forall x\left(\varphi(x) = \frac{k}{k-1}x\right)$ к языку машин Тьюринга. Пусть н. а. θ над A $(A \supset \{0, 1\})$ — фиксированное в § 1 взаимно-однозначное отображение множества слов в $\{0, 1\}$ на множество слов в A. Пусть м. т. R_θ, $R_{\theta^{-1}}$, R_U, с внешним алфавитом A, с начальными состояниями q'_θ, $q'_{\theta^{-1}}$, q'_U и с заключительными состояниями q^{*}_θ, $q^{*}_{\theta^{-1}}$, q^{*}_U таковы, что для машинных слов, описывающих состояния машин, выполнены следующие условия:

1) для машины Тьюринга $R_{\theta^{-1}}$ выполнено: для любого слова P в A

$$\exists i \, \forall z_1 z_2 \, \exists y_1 y_2 \, (a_0^{z_1} q'_{\theta^{-1}} P a_0^{z_2})^i = a_0^{y_1} q^{*}_{\theta^{-1}} \theta^{-1}(P) \, a_0^{y_2}$$

2) для м. т. R_θ выполнено:

$$\forall x \exists i \forall z_1 z_2 \exists y_1 y_2 (a_0^{z_1} q_\theta' x a_0^{z_2})^i = a_0^{y_1} q_\theta'' \theta(x) a_0^{y_2}$$

3) для м. т. R_U выполнено:

$$\forall xy (! U(x, y) \supset \exists i \forall z_1 z_2 \exists y_1 y_2 (a_0^{z_1} q_U' x a_0 y a_0^{z_2})^i =$$

$$= a_0^{y_1} q_U'' U(x, y) a_0^{y_2} \& (\neg ! U(x, y) \supset \exists i \exists P \exists Q ((q' x a_0 y)^i = P q_U'' Q).$$

(Здесь P и Q — переменные, допустимыми значениями которых являются слова в алфавите A).

Возможность построения R_θ, $R_{\theta-1}$, R_U очевидна. Пользуясь результатами работ [5] и [14], построим н. а., перерабатывающий каждое натуральное n в шифр машины W_n, такой, что

$$D(W_n^{\text{ш}}) \lesssim \frac{l(n)}{(k-1)\, l(l(n))}, \tag{2.1.4}$$

и

$$\forall x \exists i \forall z_1 z_2 \exists y_1 y_2 ((a_0^{z_1} q_n' x a_0^{z_2})^i = a_0^{y_1} q_n'' n a_0 x_0^{y_2}).$$

(Здесь q_n' и q_n'' суть начальное и заключительное состояния машины W_n).

Пусть м. т. Π_n есть композит м. т. $R_{\theta-1} * W_n * R_U * R_\theta$. (Композит м. т. понимается так же, как в [7]). Как нетрудно убедиться, если $\widetilde{U}(n \square x) = y$, то

$$\Pi_n(\theta(x)) = \theta(y) = \theta(\widetilde{U}(n \square x)) \tag{2.1.2}$$

Как следует из (2.1.1) для любого слова P в A имеет место

$$V(\Pi_n^{\text{ш}} \square P) \simeq \overline{\Pi}(P). \tag{2.1.3}$$

Из (2.1.2) и (2.1.3) следует

$$\forall n \forall x (\theta(\widetilde{U}(n \square x)) \simeq V(\Pi_n^{\text{ш}} \square \theta(x))$$

Построим транслятор T из $Я_1$ в $Я_2$, такой, что всегда $T(n) = \Pi_n^{\text{ш}}$. Имеем

$$\theta(U(n \square x)) \simeq V(T(n) \square \theta(x)),$$

Убедимся, что транслятор T φ-сводит $Я_1$ к $Я_2$, где $\varphi(x) = \frac{k}{k-1} x$.

Через δ обозначим арифметическую функцию, такую, что для любого натурального m, $\delta(m)$ равно числу м. т. со сложностью, меньшей или равной m. Как следует из [5] и [14].

$$l(\delta(m)) \lesssim l(m^{km}). \tag{2.1.5}$$

Так как с ростом сложности м. т. растет и длина их шифров (поскольку сообщения в языке машин Тьюринга нумеруются в порядке возрастания длин), то из (2.1.5) следует, что для сообщений языка машин Тьюринга имеет место

$$\forall\varepsilon\,\exists d\,\forall X\,(D(X) > d \supset L(X) < (1+\varepsilon)\,D(X)\,kl\,(D(X))). \quad (2.1.6)$$

Учитывая, что $D(W_n^{ш})$ и $D(\Pi^{ш})$ отличаются на константу и $\Pi_n^{ш}$ есть $T(n)$, из 2.1.4 получаем

$$\forall\varepsilon\,\mathrm{E}d\,\forall n\,(l(n) > d \supset D(T(n)) < (1+\varepsilon)\,\frac{l(n)}{(k-1)\,l\,(l(n))}\cdot \quad (2.1.7)$$

Из построения транслятора T имеем

$$\forall d\,\exists m\,\forall n\,(n > m \supset D(T(n)) > d). \quad (2.1.8)$$

Из (2.1.6) и (2.1.8) имеем

$$\forall\varepsilon\,\exists m\,\forall n\,(n > m \supset L(T(n)) < (1+\varepsilon)\,D(T(n))\,kl\,(D(T(n))). \quad (2.1.9)$$

Нетрудно убедиться, что из (2.1.7) и (2.1.9) будем иметь

$$\forall\varepsilon\,\exists b\,\forall n\left(l(n) > b \supset L(T(n)) < (1+\varepsilon)\,\frac{k}{k-1}\,l(n)\right).$$

Но так стандартная мера сложности L языка $Я$ есть $L(n) = l(n)$ (сообщения $Я_1$ суть натуральные числа) имеем, что $Я_1$ φ-сводится к $Я$.

Убедимся, что функция $\varphi(x) = \dfrac{k}{k-1}\,x$ есть функция плотности языка машин Тьюринга. С учетом леммы 1.1.3 достаточно доказать, что она миноранта. Пусть $\overline{D}$ — арифметическая функция, такая, что для любого натурального b $\overline{D}(b) = \max\limits_{L(X) < b} D(X)$. Из [5] и [14] имеем

$$l\,(\lambda_Я\,(b)) \lesssim l\,(\overline{D}\,(b)^{(k-1)\overline{D}(b)}. \quad (2.1.9)$$

Из определения функций $\overline{D}$ и δ имеем

$$l\,(\delta\,(\overline{D}\,(b) \dot{-} 1)) \leqslant b + 1. \quad (2.1.10)$$

Из (2.1.10) и из очевидного неравенства $\delta\,(m) \geqslant (k\,(m-1))^{km}$ следует

$$l\,(\overline{D}\,(b)^{k\overline{D}(b)}) \lesssim l\,(\delta(\overline{D}\,(b) - 1)) < b + 1, \quad (2.1.11)$$

или

$$l\,(\overline{D}\,(b)^{k\overline{D}(b)}) \lesssim b, \quad (2.1.12)$$

или

$$\frac{k-1}{k}\,(l\,(\overline{D}\,(b)^{k\overline{D}(b)}) \lesssim \frac{k-1}{k}\,b. \quad (2.1.13)$$

Из (2.1.9) и (2.1.13) имеем

$$l\,(\lambda_Я\,(b)) \lesssim \frac{k-1}{k}\,b. \quad (2.1.14)$$

Зафиксируем некоторое рациональное ε, тогда (2.1.14) для $b = \frac{k}{k-1}(1-\varepsilon)\cdot m$ имеет вид

$$l\left(\lambda_Я\left((1-\varepsilon)\frac{k}{k-1}m\right)\right) \lesssim (1-\varepsilon)\, m. \tag{2.1.15}$$

Для достаточно больших m имеем

$$l\left(\lambda_Я\left((1-\varepsilon)\frac{k}{k-1}m\right)\right) < m, \tag{2.1.16}$$

что и доказывает, что функция $\varphi(m) = \frac{k}{k-1}m$ есть миноранта.

Через $Ч$ обозначим множество всех ч. р. ф.

Следствие 2.1.1. *Язык м. т. Я с параметром k есть φ-мощностной для Ч-множеств по стандартной мере сложности $L^Я$ и* $\varphi(n) = \frac{k}{k-1}n$.

Другими словами, для любого р. п. множества M булевых функций

$$L_M^Я(n) \cong \frac{k}{k-1}\, l(d_M(n)).$$

Лемма 2.1.1. *Для языка м. т. с параметром k выполнено*

$$D(X) \sim \gamma(L(X)) \quad \text{при} \quad L(X) \to \infty,$$

где $\gamma(n) = \frac{n}{k \cdot l(n)}$.

Доказательство. Убедимся в том, что имеет место

$$L(X) \sim D(X)\, kl(D(X)), \tag{2.1.17}$$

или, иначе говоря,

$$\forall \varepsilon\, \exists d\, \forall X\, (D(X) > d \supset L(X) < (1+\varepsilon)\, D(X)\, kl(D(X))) \tag{2.1.18}$$

и

$$\forall \varepsilon\, \exists d\, \forall X\, (D(X) > d \supset L(X) > (1-\varepsilon)\, D(X)\, kl(D(X))). \tag{2.1.19}$$

Но (2.1.18) есть (2.1.6). (2.1.19) следует из неравенства $\delta(m) > (k(m-1))^{km}$.

Из (2.1.17) имеем $D(X) \sim \frac{L(X)}{kl(L(X))}$, что и требовалось. Из теоремы 1.3.2, следствия 2.1.1 и леммы 2.1.1 имеем:

Теорема 2.1.2. *Язык м. т. с параметром k является ψ-мощностным для Ч-множеств по мере сложности D, где*

$$\psi(n) = \frac{n}{(k-1)\, l(n)}.$$

Иначе говоря, для любого р. п. множества M б. ф.

$$D_M^Я(n) \cong \frac{l(d_M(n))}{(k-1)\, l(l(d_M(n)))}.$$

2°. Приведем определения языка нормальных алгоритмов (ЯНА) из [10]. Пусть $A = \{a_1, \dots, a_k\}$ — некоторый алфавит из k букв, $t_1, \dots, t_5$ — различные буквы, не входящие в A; Ξ — множество изображений правильных [5] н. а. в алфавите $A \cup \{t_4, t_5\}$ (см. [8]); V — универсальный н. а. над алфавитом $A \cup \{t_1, \dots, t_5, \square\}$ для н. а. в $A \cup \{t_4, t_5\}$. Список

$$\langle A,\ A \cup \{t_1, \dots, t_5\},\ \Xi,\ V \rangle$$

будем называть ЯНА. Натуральное число k, равное мощности алфавита A, будем называть параметром ЯНА. Для ЯНА определим н. а. D над $A \cup \{t_4, t_5, 0, \mid\}$ такой, что для любого сообщения X (изображения н. а. в $A \cup \{t_4, t_5\}$) $D(X) = X^\partial$.

Нетрудно убедиться, что D есть мера сложности для ЯНА.

В [10] доказывается, что всякий ЯНА асимптотически оптимален и, следовательно, имеет место.

Следствие 2.2.1. *ЯНА φ-мощностной для Ч-множеств по стандартной мере $L^Я$, где $\varphi(n) = n$.*

Из [5] и [10] имеем

Лемма 2.2.1. *Для ЯНА с параметром k выполнено*

$$D(X) \sim \gamma(L(X)),$$

где $\gamma(n) = \dfrac{n}{\log k}$.

Следствие 2.2.2. *ЯНА с параметром k ψ-мощностной для Ч-множеств по мере сложности D, где $\psi(n) = \dfrac{n}{\log k}$, иначе говоря, для любого р. п. множества M б. ф.*

$$D_M^Я(n) \cong \frac{l(d_M(n))}{\log k}.$$

3°. Пусть K — некоторый класс ч. р. ф., содержащий E^3 и замкнутый относительно подстановок и ограниченного минимума. Пусть K_1 и K_2 соответственно классы одноместных и двуместных функций из K, и пусть U — двухместная ч. р. ф., универсальная для K_1. Согласно [4] и [2] (см. например, теоремы 4 и 5 из [2]), пользуясь U, можно построить двухместную ч. р. ф. A, такую, что для всякой ч. р. ф. F из K_2 существует о. р. ф. δ и константа C, удовлетворяющие условиям

$$A(\delta(n), x) \simeq F(n, x) \quad \text{и} \quad l(\delta(n)) < l(n) + C.$$

Функцию A, удовлетворяющую вышеуказанным условиям, будем называть аддитивно оптимальной для класса K_2. Через $\overline{K}_2$, как прежде, будем обозначать класс алгорифмических языков, ассоциированных с функциями F из K_2 (см. (1.2.1)). Нетрудно убедиться, что если A аддитивно оптимальна для класса K_2, то алгорифмический язык, ассоциированный с A, φ-равномерен относительно $\overline{K}_2$ и $\varphi(x) = x$. Тогда из теоремы 1.2.2 имеем

Следствие. *Пусть K — класс ч. р. ф., содержащий E^3 и замкнутый относительно подстановок и ограниченного минимума; пусть A — аддитивно оптимальная функция для K_2 и Я — алгорифмический язык, ассоциированный с A. Тогда Я является φ-мощностным для K-множеств б. ф. (где $\varphi(x) = x$).*

Замечание. Если в качестве класса K взять, например, класс E^m — m-ый класс п. р. ф. в иерархии Гжегорчика ($m \geqslant 3$) и если аддитивно оптимальная функция A для E_2^m принадлежит классу E_2^{m+i} ($i \geqslant 1$), то алгорифмический язык Я, ассоциированный с A, будет φ-мощностным (с $\varphi(x) = x$) для E^m-множеств б. ф. и не будет φ-мощностным для E^{m+i}-множеств б. ф..

Факты, аналогичные сформулированным в этом замечании, имеют место и для других иерархий о. р. ф.

Հ. Հ. ՆԱԶԱՐՅԱՆ

ԱԼԳՈՐԻԹՄԻԿ ԼԵԶՈՒՆԵՐՈՒՄ ԲՈՒԼՅԱՆ ՖՈՒՆԿՑԻԱՆԵՐԻ ԻՐԱՑՄԱՆ ՄԱՍԻՆ

Ա մ փ ո փ ո ւ մ

Դիտարկվում է այս կամ այն դասին պատկանող բուլյան ֆունկցիաների իրացումների բարդությունների գնահատականները տարբեր ալգորիթմիկ լեզուներում։ Հիմնական ուշադրությունը նվիրվում է այն բանի որոշելուն, թե բուլյան ֆունկցիաների որ դասերի համար և որ ալգորիթմիկ լեզուներում հնարավոր է ստանալ լավագույն (ասիմպտոտիկ իմաստով) հզորական գնահատականներ իրացումների բարդությունների համար։

ЛИТЕРАТУРА

1. *Гельфонд М. Г.* О конструктивных псевдофункциях. Зап. научн. семинаров. Ленинград. отд. ин-та АН СССР, т. 16, 20—28 (1969).
2. *Заславский И. Д.* О псевдофункциях Шеннона. Зап. научн. семинаров Ленингр. отд. Матем. ин-та АН СССР, т. 16, 65—76 (1969).
3. *Звонкин А. К., Левин Л. А.* Сложность конечных объектов и обоснование понятий информации и случайности с помощью теории алгоритмов. УМН XXV 6, 85—127, (1970).
4. *Колмогоров А. Н.* Три подхода к определению понятия «количество информации». Проблемы передачи информации, 1, 1, 3—7 (1965).

5. *Кузьмин В. А.* Реализация функций алгебры логики автоматами, нормальными алгорифмами и машинами Тьюринга. Сб., «Проблемы кибернетики», вып. 13, 75—96 (1965).
6. *Лупанов О. Б.* Об одном подходе к синтезу управляющих систем—принципе локального кодирования. Сб. «Проблемы кибернетики», вып. 14, М., «Наука», 1965, 31—111.
7. *Мальцев А. И.* Алгоритмы и рекурсивные функции. М., «Наука», 1965.
8. *Марков А. А.* О конструктивных функциях. Труды МИАН СССР им. В. Стеклова. т. 52, 315—348, (1958).
9. *Марков А. А.* Теория алгорифмов. Труды МИАН СССР им. В. Стеклова, т. 42, 1954.
10. *Тер-Захарян Н. П.* О некоторых количественных характеристиках алгорифмических языков. ДАН 190, 3, 538—540 (1970).
11. *Шанин Н. А.* Конструктивные вещественные числа и конструктивные функциональные пространства. Труды МИАН им. В. Стеклова, 67, 15—294, (1962).
12. *Шанин Н. А.* О конструктивном понимании математических суждений. Труды Мат. ин-та им. В. А. Стеклова, т. 52, 226—311, (1958).
13. *Яблонский С. В.* Об алгоритмических трудностях синтеза минимальных контактных схем, сб. «Проблемы кибернетики» вып. 2, 75—123, (1959).
14. *Chaitin G. Z.* On the lengh of programs for computing finite binary sequences JACM, 13, 547—570, (1966).
15. *Grzegorczyk A.* Some classes of recursive functions. Rozpr. Mat. 4, 1953, 1—45. (Русский перевод: *А. Гжегорчик.* Некоторые классы рекурсивных функций. „Проблемы математической логики". „Мир", М., 9—49 (1970).
16. *Blum M.* On the size of machines, Information and Control, 11, № 3, 257—265, (1967). (Русский перевод: *Блюм М.,* Об объеме машин. Проблемы математической логики, „Мир", М., 423—431).