ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LV 1972 3

УДК 510.164

МАТЕМАТИКА

Г. А. Назарян

Некоторые оценки реализации булевых функций в алгорифмических языках

(Представлено чл.-корр. АН Армянской ССР А. А. Талаляном 6 III 1972)

В работе рассматриваются оценки сложности реализации управляющими системами булевых функций, принадлежащих классам некоторого достаточно широкого типа (ср. [1]), а также сравниваются оценки сложности реализации булевых функций управляющими системами различных типов [2].

Суждения, формулируемые в настоящей работе, понимаются конструктивно.

Всюду далее ч. р. ф. есть сокращение для выражения „частично рекурсивная функция", б. ф. — „булева функция", н. а. — „нормальный алгорифм", м. т. — „машина Тьюринга", р. п. м. — „рекурсивно перечислимое множество".

Определим натуральные числа как слова в алфавите $A_0 = \{0,1\}$. При этом роль нуля играет пустое слово, а роль операции следования — алгорифм F такой, что для любого слова p в A_0, $F(\Lambda) = 0$, $F(p0) = p1$, $F(p1) = F(p)0$ (ср. [3]). Длину натурального числа x обозначим через $l(x)$. Для конкретных натуральных чисел сохраним обозначения 0, 1, 2, . . . Зафиксируем некоторую двуместную асимптотически оптимальную ч. р. ф., например, функцию $A(n, x)$, построенную в [4]. Для положительных натуральных чисел будем рассматривать условную сложность вида $K(x|l(x))$ (см. [4]) относительно A. Ее можно определить как всюду определенную двуместную псевдофункцию [4-6]. Согласно [4] и [5] (см., например, теоремы 4 и 5 из [5]) можно построить двуместную ч. р. ф. V, универсальную для всех одноместных ч. р. ф., и такую, что для всякой двуместной ч. р. ф. V_1 существуют одноместная общерекурсивная функция φ и константа C, удовлетворяющие условиям: $V(\varphi(n), x) \simeq V_1(n, x)$ и $l(\varphi(n)) < l(n) + C$. Через $\sigma_i(p)$, где i — натуральное число, не превосходящее длины натурального числа p, будем обозначать однобуквенное слово, единственная буква которого совпадает с i-той буквой слова p, начиная слева (при этом нумерацию букв начинаем с единицы. Через φ обозначим арифметическую функцию, такую, что всегда $\varphi(n)=\frac{n(n-1)}{2}$. Говорим, что двуместная ч. р. ф. E смещенно разрешает положительное натуральное число x при натуральном числе p, если $E(p, \varphi(l(x))+i)=\xi_i(x)$ при $1 \leq i \leq l(x)$.

Для всякой двуместной ч. р. ф. E введем в рассмотрение псевдофункцию KRS_E следующим образом: $KRS_E(x)=y$ имеет место в том и только в том случае, когда

$$\neg\neg\exists p(E(p, \varphi(l(x)+i)=\xi_i(x) \& l(p)=y \&$$

$$\& \neg\exists q(l(q)<y \& E(q, \varphi(l(x))+i)=\xi_i(x).$$

Натуральное число y, удовлетворяющее указанному условию, будем называть сложностью смещенного разрешения слова x относительно E. Сложностью смещенного разрешения KRS слова x назовем сложность его смещенного разрешения относительно функции U.

Следующая лемма устанавливает связь между величинами $K(x|l(x))$ и $KRS(x)$ (ср. (7), теоремы 2.2 и 2.3).

Лемма. *Существует натуральное число C такое, что для любого положительного натурального x*

$$|K(x|l(x)) - KRS(x)| \leq C.$$

Через ν будем обозначать арифметическую функцию, такую, что всегда $\nu(x)=\sum_{k=1}^{l(x)} \xi_k(x)2^{l(x)-k}$. Всякое натуральное число f длины 2^n будем называть булевой функцией от n переменных. Значением б. ф. f от n переменных на натуральном числе x длины n будем называть число $\xi_{\nu(x)}(f)$, которое будем обозначать через $f(x)$.

Пусть M — рекурсивно перечислимое множество б. ф., тогда через M_n будем обозначать множество б. ф. от n переменных, принадлежащих M. При фиксированном M посредством d_M будем обозначать одноместную псевдофункцию, такую, что для всякого n значением $d_M(n)$ этой псевдофункции является количество б. ф., принадлежащих M_n. (Строгое определение этой псевдофункции дается очевидным образом). Далее мы будем пользоваться понятиями и определениями, введенными в (3). Зафиксируем некоторый асимптотически оптимальный язык Я $=\langle A_j, A_i, \Omega, V\rangle$ с критерием сложности L. Будем говорить, что сообщение X языка Я реализует б. ф. f от n переменных и писать $X \underset{Я}{\Rightarrow} f$, если для любого слова P в A_0 длины n имеет место $V(X \square P)=f(P)$. Пусть псевдофункция L_M определяется следующим образом: $L_M(n)=z$ в том и только в том случае, если

$$\forall f(f\in M_n \supset \neg\neg\exists X(X \underset{Я}{\Rightarrow} f \& L(X)\leq z) \&$$

$$\& \forall z'(z'<z \supset \neg\neg\exists f(f\in M_n \& \forall X(X \underset{Я}{\Rightarrow} f \supset L(X)>z')).$$

Если A и B какие-либо псевдофункции, определенные для натуральных чисел и принимающие натуральные значения, то через $A(n) \underset{n\to\infty}{\to} \infty$ будем обозначать суждение $\forall m \exists n \forall k (k > n \supset A(k) > m)$, а через $A(n) \underset{n\to\infty}{\sim} B(n)$ будем обозначать суждение

$$\forall m \exists n \forall k (k > n \supset B(k) \neq 0 \,\&\, \left| \frac{A(k)}{B(k)} - 1 \right| < 2^{-m}).$$

Теорема 1. *Для всякого р. п. м. M и для всякого асимптотически оптимального языка $\mathfrak{Я}$ оказывается*

1) если $d_{м}(n) \underset{n\to\infty}{\to} \infty$, то $L_{м}(n) \sim l d_{м}(n)$;

2) если $\exists C \forall_n (d_{м}(n) < C_1)$, то $\exists C \forall_n (L_{м}(n) < C)$.

Зафиксируем алфавит $A = \{a_1, \ldots, a_k\}$ из k букв, где $a_1 = 0$ и $a_2 = 1$. Будем рассматривать нормальные алгорифмы в алфавите A. Нижеследующие два определения совпадают с соответствующими определениями в работе ([8]). Будем говорить, что н. а. Q в A реализует б. ф. f от n переменных, и писать $Q \underset{н}{\succ} f$, если для любого натурального числа p длины n $Q(p) = f(p)$. Сложностью н. а. Q назовем длину его изображения $|Q|^{н.а.}$ ([9]). Пусть одноместная псевдофункция $D^k_{м}$ определяется следующим образом: $D^k_{м}(n) = z$ имеет место тогда и только тогда, когда

$$\forall f (f \in M_n \supset \neg\neg \exists Q (Q \underset{н}{\succ} f \,\&\, |Q|^{н.а.} \leq z) \,\& \tag{1}$$

$$\& \,\forall z' (z' < z \supset \neg\neg \exists f (f \in M_n \,\&\, \forall Q (Q \underset{н}{\succ} f \supset |Q|^{н.а.} > z')))).$$

Язык нормальных алгорифмов мы определим так же, как в ([3]) (в частности, так же, как и в ([3]), мы рассматриваем только правильные н. а. ([10])). В ([3]) показано, что язык нормальных алгорифмов асимптотически оптимален, а следовательно, для него верна теорема 1. Применяя ее, получаем следующую теорему.

Теорема 2. *Для всякого р. п. м. M булевых функций оказывается*

1) если $d_{м}(n) \underset{n\to\infty}{\to} \infty$, то $D^k_{м}(n) \underset{n\to\infty}{\sim} \dfrac{l d_{м}(n)}{\log k}$;

2) если $\exists C_1 \forall n (d_{м}(n) < C_1)$, то $\exists C \forall n (D^k_{м}(n) < C)$.

Пусть $A = \{a_0, \ldots, a_{k-1}\}$ — некоторый фиксированный алфавит из k букв, где $a_1 = 0$, $a_2 = 1$. Будем рассматривать машину Тьюринга с внешним алфавитом A и символом пустого состояния ячейки a_0. (Все понятия, связанные с м. т., понимаются как в ([11]) (§§ 12.1, 12.2).

Будем говорить, что м. т. R вычисляет б. ф. f от n переменных, и писать $R \underset{т}{\succ} f$, если для любого натурального числа p длины n имеет место $\overline{R}(p)=f(p)$ (где $\overline{R}$ — программа м. т. R). Сложностью машины Тьюринга назовем число ее внутренних состояний ([10, 12]); сложность машины Тьюринга R будем обозначать через $N(R)$. Введем псевдофункцию D^k_M аналогично (1), а именно: $D^k_M(n)=z$ имеет место в том и только в том случае, если

$$\forall f(f\in M_n \supset \neg\neg\exists R(R \underset{\text{т}}{\succ} f \,\&\, N(R)\leq z)\,\&$$

$$\&\,\forall z'(z'<z \supset \neg\neg\exists f(f\in M_n \,\&\, \forall R(R \underset{\text{т}}{\succ} f \supset N(R)>z'))).$$

Теорема 3. *Для всякого р. п. м. М булевых функций оказывается*

1) если $d_M(n) \underset{n\to\infty}{\to} \infty$, *то* $D^k_M(n) \sim \dfrac{l d_M(n)}{(k-1)ll d_M(n)}$;

2) если $\exists C_1 \forall n(d_M(n)\leq C_1)$, *то* $\exists C\forall n(D^k_M(n)<C)$.

Пусть Я $=\langle A_j, A_l, \Omega, V\rangle$ — некоторый алгорифмический язык с критерием сложности L и $A_j\supset\{0, 1\}$.

Говорим, что язык Я булевски разрешим, если существует н. а. G над $A_j\cup\{\square\}\cup A_l$, применимый к любому слову вида $X\square f$, где X — сообщение языка Я, f — б. ф., и такой, что $G(X\square f)=\Lambda$ в том и только в том случае, когда сообщение X реализует б. ф. f.

Введем одноместную псевдофункцию $\overline{L}$ следующим образом: если f не есть б. ф., то $\overline{L}(f)=0$; если f есть б. ф. то $\overline{L}(f)=z$ в том и только в том случае, если $\neg\neg\exists X(X \underset{\text{Я}}{\succ} f \,\&\, L(X)=z)\,\&\,\forall X(X \underset{\text{Я}}{\succ} f\supset L(X)\geq z)$. (В нижеследующей теореме 4 посредством $\overline{L}^{(1)}$ и $\overline{L}^{(2)}$ обозначены псевдофункции, построенные только что указанным образом для языков, соответственно, Я$_1$ и Я$_2$). Всякую псевдофункцию, определенную для любых натуральных чисел, условимся называть псевдопоследовательностью. Через F обозначим множество всех б. ф.

Теорема 4. *Пусть Я$_1$ — булевски разрешимый язык с критерием сложности L^1 и Я$_2$ — асимптотически оптимальный язык с критерием сложности L^2. Пусть для некоторого р. п. м. М булевых функций такого, что* $d_M(n) \underset{n\to\infty}{\to} \infty$, *имеет место* $L^1_M(n)/L^1_l(n)\to 0$. *Тогда существуют две псевдопоследовательности* $\{\varphi_i\}$ *и* $\{\psi_i\}$ *б. ф. таких, что при любом i функции* φ_i *и* ψ_i *зависят от i аргументов, и имеют место соотношения* $\overline{L}^{(1)}(\varphi_i)/\overline{L}^{(1)}(\psi_i)\to 0$ *и* $\overline{L}^{(2)}(\varphi_i)/\overline{L}^{(2)}(\psi_i)\to\infty$ *при* $i\to\infty$.

Легко видеть, что условия теоремы 4 будут выполнены, если в роли языка Я$_1$ мы будем рассматривать такие языки, как, например, язык контактных схем, язык функциональных схем в данном базисе, язык примитивно рекурсивных функций и т. п. (соответствующие определения в рамках понятия алгорифмического языка из ([3]) даются естественным образом (ср., например, ([3]), п. 4)). Таким образом мы можем заключить из теоремы 4, что квазносуществимы булевые функции, достаточно просто реализуемые с помощью, например, нормальных алгорифмов и достаточно сложно реализуемые с помощью контактных схем, функциональных схем или примитивно рекурсивных функций.

В заключение пользуюсь случаем выразить глубокую благодарность Н. Д. Заславскому, под руководством которого выполнена настоящая работа. Я также глубоко признателен Н. П. Тер-Захаряну и Г. Б. Маранджяну за ряд ценных советов и замечаний.

Вычислительный центр Академии наук
Армянской ССР и Ереванского государственного
университета

Հ. Հ. ՆԱԶԱՐՅԱՆ

Ալգորիթմիկ լեզուներում բուլյան ֆունկցիաների իրականացման մի քանի գնահատականներ

Դիտարկվում են տարբեր ալգորիթմիկ լեզուներում ռեկուրսիվ թվարկելի դասերին պատկանող բուլյան ֆունկցիաների իրականացման բարդության հետ կապված հարցերը։

Ապացուցվում է, որ ալգորիթմիկ լեզուների լայն դասում՝ մասնավորապես ցանկացած ասիմպտոտիկ օպտիմալ լեզվում, բուլյան ֆունկցիաների ամեն մի ռեկուրսիվ թվարկելի դասի համար տեղի ունեն բուլյան ֆունկցիաների իրականացման բարդության հզորական գնահատականներ (տեխնիկական բնույթի լրացուցիչ պայմանների կատարման դեպքում)։

Մտցվում է բուլյան լուծելի լեզվի գաղափարը (այդպիսի լեզուներից են օրինակ՝ տվյալ բազիսում ֆունկցիոնալ սխեմաների լեզուն, կոնտակտային սխեմաների լեզուն) և ապացուցվում է, որ կամայական ասիմպտոտիկ օպտիմալ $Я_1$ լեզվի և կամայական բուլյան լուծելի $Я_2$ լեզվի համար չեն կարող գոյություն չունենալ բուլյան ֆունկցիաներ, որոնց համար $Я_1$-ում և $Я_2$-ում իրականացման բարդությունների հարաբերությունը լինի կամայական ձևով մեծ։

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *С. В. Яблонский*, Об алгоритмических трудностях синтеза минимальных контактных схем, ПКЗ, 75—123, (1959). [2] *Н. Д. Заславский*, ДАН Арм. ССР, т. XLVII, № 3 (1968). [3] *Н. П. Тер-Захарян*, ДАН 190, 3, 538—540, (1970). [4] *А. Н. Колмогоров*, Проблемы передачи информации, I, 1, 3—7, (1965). [5] *Н. Д. Заславский*, Зап. научн. семинаров Ленингр. отд. Матем. ин-та АН СССР, т. 16, 65—76 (1969). [6] *М. Г. Гельфонд*, Зап. научн. семинаров Ленингр. отд. Матем. ин-та АН СССР, т. 16, 20—28. [7] *А. А. Звонкин, Л. А. Левин*, УМН 25:2, 85, (1970). [8] *А. А. Марков*, Известия АН, сер. матем. 31 (1967). [9] *А. А. Марков*, Труды МИАМН СССР им. В. Стеклова, XLII, (1954). [10] *В. А. Кузьмин*, Реализация функций алгебры логики автоматами, нормальными алгорифмами и машинами Тьюринга, ПК 13, (1969). [11] *А. И. Мальцев*, Алгоритмы и рекурсивные функции, «Наука», М., (1965). [12] *G. J. Chaitin*, Journ. Assoc. Comp. Mach. 13, 547—570, (1966).