ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXIII 1976 5

УДК 517.11

МАТЕМАТИКА

Г. А. Назарян

О классах сложности множеств булевых функций

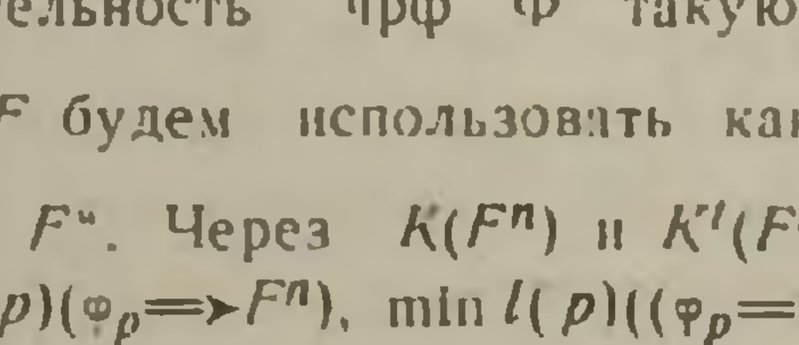
(Представлено чл.-корр. АН Армянской ССР А. А. Талаляном 29/IV 1976)

В статье рассматриваются вопросы реализации булевых функций в алгорифмических языках при ограничении на время работы алгорифмов, а также классы сложности множеств булевых функций.

1. Всюду далее орф есть сокращение для выражения „общерекурсивная функция", чрф — „частично рекурсивная функция", рпм — „рекурсивно перечислимое множество", н. ч.— „натуральное число", б. ф.— „булева функция".

Определим н. ч. как слова в алфавите $\{0, 1\}$, так же как в [1]. Булевы функции и связанные с ними понятия, здесь не определяемые, будем понимать естественным образом, например как в [2], в частности б. ф. размерности n рассматривается как слово длины 2^n в алфавите $\{0, 1\}$ (н. ч.). Через $l(x)$ будем обозначать длину н. ч. x, $d(A)$ — мощность конечного множества A. Размерность б. ф. будем указывать верхним индексом. Посредством M_n будем обозначать множество б. ф. размерности n, принадлежащих множеству M. Буквой G будем обозначать класс всех б. ф. Буквы t, T, τ (возможно с индексами) будем использовать для обозначения одноместных орф, M — для множества б. ф., F, P — для б. ф., C, p — для н. ч.

Зафиксируем некоторую аддитивно оптимальную нумерацию [3,4] чрф φ. Для нумерации φ зафиксируем конструктивную последовательность сигнализирующих Ф, с последовательностью сигнализирующих Ф ассоциируем последовательность чрф $\hat{\Phi}$ такую, что $\forall i \forall n(\hat{\Phi}_i(n) = \max\limits_{l(x)=n} \Phi_i(x))$. Запись $\alpha \Longrightarrow F$ будем использовать как сокращение для „чрф α вычисляет б. ф. F^n". Через $K(F^n)$ и $K^t(F^n)$ будем обозначать соответственно $\min l(p)(\varphi_p \Longrightarrow F^n)$, $\min l(p)((\varphi_p \Longrightarrow F^n)\,\&\,(\Phi_p(n) < t(n)))$ и через L_M и L^t_M соответственно $\max\limits_{F^n \in M_n} K(F^n)$ и $\max\limits_{F^n \in M_n} K^t(F^n)$. Символы $\dot{\geq}$, $\dot{\leq}$ и $\dot{=}$ используются в следующем смысле: $a(n) \dot{\geq} b(n) \equiv \exists C \forall n(a(n) + C > b(n))$, $a(n) \dot{\leq} b(n) \equiv \exists C \forall n(a(n) < b(n) + C)$ и $a(n) \dot{=} b(n) \equiv a(n) \dot{\geq} b(n)\,\&\,a(n) \dot{\leq} b(n)$. Множество M б. ф. будем



называть T-мощностным, если выполнено $\exists t(L^t_M \succeq L_M \succeq l(d(M_n)))$ (нетрудно убедиться, что если M рпм, то $L_M \succeq l(d(M_n))$. В дальнейшем рассматривая поведение произвольной сигнализирующей будем иногда для краткости называть ее „время вычислений" или просто „время", под „объемом программы" будем понимать индекс p нумерации φ.

2. Следующее довольно очевидное утверждение (2.1) показывает существование множеств, допускающих „ускорения" вычислений б. ф. им принадлежащим только при существенном увеличении объема программ их вычисляющих. Утверждение 2.2 иллюстрирует возможность обратной картины—существование множеств допускающих „ускорения" вычислений б. ф. им принадлежащих при незначительном увеличении объемов программ. В 2.1 и 2.2 M—рекурсивное множество.

2.1 $$\forall t \exists M \exists C \exists t_1((L^t_M < C) \;\&\; (L^{t_1}_M \geqslant 2^n)).$$

2.2 $$\exists t_0 \forall t_1 \exists M \exists C_1 \exists C_0 \exists t > t_1((L^t_M(n) \leqslant C_1) \;\&\; \forall \bar{t}|(\bar{L}^{\bar{t}}_M(n) < C_1) \supset \forall^\infty n(t(n) > t_1(n))| \;\&\; \forall^\infty n(L^t_M(n) < C_0)).$$

Множество б. ф. будем называть S—множеством, где S—некоторый класс орф, если характеристическая функция этого множества принадлежит S.

2.3. *Для всякого перечислимого класса S орф можно указать t такую, что для любого S-множества M выполнено $L^t_M \succeq L_M$.*

Нетрудно убедиться, что всякое рекурсивное множество является T-мощностным, т. е. $\exists t(L^t_M \succeq L_M \succeq ld(M_n))$ (это следует например из 2.3). Иначе „ведут" себя рпм. Как будет показано в дальнейшем для них функции Шеннона L и L^t могут существенно отличаться при любых t. Но сложность множества L^t_M определяется сложностью „сечений"—M_n. Одной из возможных характеристик сложности „сечений" является сложность их характеристических функций. Через i_{M_n} будем обозначать характеристический вектор множества M_n—вектор $\sigma_1 \sigma_2 \cdot \cdot \cdot \sigma_{2^n}$, i-ая буква которого равна 1 если F^n_i (i-ая б. ф. в лексикографической упорядоченности среди б. ф. размерности n) принадлежит M. Будем рассматривать условную сложность ([3]) $K^t(i_{M_n}|n) = \mu p|\varphi_p(n) = i_{M_n} \;\&\; \Phi_p(n) < t(n)|$. Как показывает следующее утверждение, ограниченность функции $K^t(i_{M_n}|n)$ при подходящей t является достаточным условием (но не необходимым—см. 2.6) для того, чтобы множество было T-мощностным.

2.4 $$\forall t_1 \exists t_2 \forall M|L^{t_2}_M(n) \leqslant 2K^{t_1}(i_{M_n}|n) + ld(M_n)|.$$

Как следует из 2.4, множество M, задаваемое схемой $\forall n(M_n = M'_n$ если $lP_l(n))$ (где M^l $(l = 1, \cdot \cdot \cdot, k)$—некоторые рекурсивные мно-

жества, и P_i ($i=1, \cdot\ \cdot\ \cdot, k$)—частично рекурсивные предикаты с непересекающимися областями определения), является T-мощностным, несмотря на то, что может быть не рекурсивным.

Введем некоторые определения. Множества M и M' будем называть аддитивно равномощными, если $l(d(M_n)) \asymp l(d(M'_n))$. Множество M будем называть (n, l)—восстанавливаемым, если $\exists t \exists C(K^t(\nu_{M_n}| < n, ld(M_n)>) < C)$. Пусть D_x обозначает конечное множество н. ч. с каноническим номером x ([3]). Орф g будем называть правильной, если для всех n и m $D_{g(n, m)}$ суть множества б. ф. и выполнено $(m_1 \leqslant m_2 \supset D_{g(n, m_1)} \subseteq D_{g(n, m_2)})$. Пусть α-орф, удовлетворяющая условию $\forall n(\alpha(n) \geqslant 2^{2^n})$. Правильную орф g будем называть функцией покрытия для M если $\forall n \neg\neg \exists m \leqslant \alpha(n)\ |D_{g(n, m)} \supseteq M_n|$. Функция покрытия для M задает таким образом некоторый единый (по n) способ покрытия сечений M_n. Пусть g есть функция покрытия для M. Множество M' будем называть покрытием M по g если $\forall n(D_{g(n, m)} = M'_n)$, где m—наименьшее н. ч. такое, что $D_{g(n, m)} \supset M_n$. M' будем называть покрытием для M если M' есть покрытие M по некоторой орф g.

Следующее утверждение устанавливает некоторые необходимые и достаточные условия для того, чтобы M было T-мощностным.

2.5 *Условия* (а), (б) *и* (в) *эквивалентны, для* M:

(а) M *является* T*-мощностным,*

(б) *существует аддитивно равномощное ему* (n, l)*-восстанавливаемое надмножество* M',

(в) *существует аддитивно равномощное ему покрытие* M'.

Используя 2.5 легко доказать следующее утверждение.

2.6. *Существует* T*-мощностное* M *такое, что* $\forall t \forall C \neg(K^t(\nu_{M_n})n) < C)$.

Из 2.6 следует, что ограниченность $K^t(\nu_{M_n}|n)$ не является необходимым условием для того, чтобы M было T-мощностным.

2.7. *Пусть* M' *есть покрытие для* M, *тогда* $\exists t(L^t_M(n) \leqslant ld(M_n))$.

2.8 *Если* M' *есть покрытие для рпм* M, *тогда* M' *также рпм.*

3. В этом пункте мы сформулируем некоторые свойства множеств, очевидным образом обуславливающие скачок оценок при ограничении на время вычислений и покажем существование множеств, для которых L и L^t существенно отличаются при любых t.

Под частично рекурсивной последовательностью (чрп) б. ф. будем понимать множество значений чрф ψ, удовлетворяющей условию $!\psi(n) \supset (\psi(n)$ есть б. ф. размерности $n)$. Множество M будем называть предельным, если любая чрп S б. ф. почти содержится в M, т. е. множество $S-M$ не бесконечно.

3.1 M *предельно* $\Longleftrightarrow \min\limits_{F^n \in \overline{M}} K(F^n) \to \infty$.

На множества б. ф. естественным образом могут быть распространены понятия простоты и иммунности ([3]).

3.2. *Если рпм* M *предельно, либо выполнено* $\min\limits_{F^n \in \overline{M}} K(F^n) \to \infty$, *то*

$\forall t(L^t_M(n) \geqslant 2^n)$ *и* M *просто* (*а, следовательно,* $\overline{M}$*-иммунно*).

3.3 *Для любой неограниченной, неубывающей орф* g *можно указать простое множество* M *такое, что* $\forall t(L^t_M(n) \geqslant 2^n)$ *и* $L_M(n) \leqslant g(n)$.

В качестве искомого в 3.3 может быть выбрано множество M, удовлетворяющее условию: $\forall n(M_n = |F^n| K(F^n) < (g(n))|)$. Условия для M выполнены в силу его предельности, либо того, что $\min\limits_{F^n \in \overline{M}} K(F) \to \infty$. Орф γ будем называть мажорантой сложности для M если $\exists t(L^t_M(n) \leqslant \gamma(n))$. Довольно очевидно, что если M имеет имунное дополнение и γ есть мажоранта сложности для M, то множество $\{n | \gamma(n) < 2^n\}$ не бесконечно, с другой стороны, из факта существования сколь угодно „редких" простых множеств следует — существует простое M такое, что $\exists t \exists C \forall n \neg \neg \exists m(L^t_M(m) < C)$. Таким образом мажоранты сложности в свою очередь могут отличаться от L^t.

3.4. *Пусть рпм* M *и орф* α *удовлетворяют условию* $-\forall n(d(M_n) < \alpha(n))$ *и множество* $\{n | d(M_n) = \alpha(n)\}$ *не конечно. Тогда можно указать орф* t *и последовательность н. ч.* n_i *такие, что* $L^t_M(n_i) \leqslant L_M(n_i)$.

Функция α в условии 3.4 может быть выбрана равной константе C, тогда из 3.4 следует: (а) утверждение 3.3 не может быть усилено до такого — „$\exists M((L_M(n) < C)\ \&\ \forall t(L^t_M(n) \geqslant 2^n))$", или иначе функция g в условии 3.3 не может быть константной, (б) из 3.4 вкупе с тем, что если M просто, и γ есть мажоранта сложности для M, то $\forall^\infty_n(\gamma(n) \geqslant 2^n)$ следует, что параллельно с фактом существования сколь угодно „редких" простых множеств они обладают следующим любопытным свойством — (M — просто $\supset$ $\neg \exists C(d(M_n) < C)$.

4. Здесь мы сформулируем некоторые факты, относящиеся к сложности разрешения рпм н. ч. (ср. ([6–8])), которые представляют самостоятельный интерес, и которые позволят как следствия из них сформулировать факты о булевых функциях.

Букву Π будем использовать в качестве переменной для рпм н. ч. Под сложностью разрешения (t разрешения) n-куска рпм Π будем понимать $l(\min p)$, где min берется по всем p таким, что $\forall x(l(x) \leqslant n \supset (!\varphi_p(x)\ \&\ (x \in \Pi \Leftrightarrow \varphi_p(x) = 0)))$. $(\forall x(l(x) \leqslant n \supset (!\varphi_p(x)\ \&\ x \in \Pi \Leftrightarrow \varphi_p(x) = 0\ \&\ \Phi_p(x) \leqslant t(l(x)))$. Сложности разрешения и t разрешения n-куска рпм Π будем обозначать соответственно через $K(\Pi, n)$ и $K^t(\Pi, n, t)$. Пусть Π_n есть множество н. ч. длины n из Π и λ_{Π_n} как и в случае множеств б. ф. обозначает характеристический вектор Π_n. Следующие соотношения легко проверяются

4.1. (а) $\forall \Pi(K(\lambda_{\Pi_n} | n) \leqslant K(\Pi, n))$,

(б) $\forall t_1 \exists t_2 \forall \Pi(K^{t_2}(\lambda_{\Pi_n} | n) \leqslant K^{t_1}(\Pi, n, t_1))$,

(в) $K(\lambda_{\Pi_n} | n) \leqslant L_d(\Pi_n)$.

Пусть β—орф. П будем называть β-редким, если $\forall n(d|x|l(x)\leqslant n \;\&\; x\in \Pi \leqslant \beta(n))$. Орф g будем называть верхней оценкой сложности разрешения (сложности t разрешения) рпм П ([8]), если выполнено $K(\Pi, n)\leqslant g(n)$, $K(\Pi, n, t)\leqslant g(n)$).

4.2. *Для любой монотонной неограниченной орф g, такой, что $\forall n(g(n)<n)$ можно указать неограниченную монотонную орф β такую, что g является верхней оценкой сложности разрешения любого β-редкого рпм.*

Из 2.4 и 4.1 (б) легко следует

4.3. *(а) Пусть* П— *простое множество. Для любой орф t, для любой верхней оценки сложности t разрешения выполнено:*

$$g(n)\geqslant \frac{n}{2}-\frac{1}{2}l(d(\Pi_n)).$$

(б) *Для любой монотонной неограниченной β можно указать β-редкое рпм* П *такое, что* $\forall t(K^t(\Pi_n|n)\geqslant n/2-\beta(n)/2$.

Из 4.1—4.3 а также факта существования сколь угодно редких простых множеств следует, что верхние оценки разрешения и ограниченного разрешения рпм могут существенно отличаться. Из этих утверждений также следует

4.4. *Пусть g-неограниченная, неубывающая орф. Существует псевдопоследовательность ([9]) б. ф. F^n_n такая, что*

$$\text{(а)}\quad K(F^n_n)\leqslant g(n) \quad и \quad \text{(б)}\forall t\left(K^t(F^n_n)\geqslant \frac{n}{2}-\frac{g(n)}{2}\right).$$

В качестве искомой псевдопоследовательности может быть выбрана λ_{Π_n} некоторого достаточно редкого простого множества. Таким образом в классе псевдопоследовательностей б. ф. описуемы „естественные" псевдопоследовательности для которых $K(F^n_n)$ и $K^t(F^n_n)$ существенно отличаются при любых t.

5. Под классом сложности R_t множеств б. ф. будем понимать класс таких рпм M, для которых выполнено $L_M\supseteq L'_M$. Многие факты, относящиеся к классам сложности чрф ([10]) легко переносятся на классы сложности множеств б. ф. Так, существует равномерная процедура получения нового класса сложности, строго включающего R_t по сигнализирующей для t (5.1), в то же время из аналога теоремы о пробелах (5.2) следует невозможность такой процедуры, равномерной относительно самой t.

5.1. *Существует орф H такая, что для любого i если φ_i есть орф, то $R_{H(n,\Phi_i(n))}\supset R_{\varphi_i}$.*

5.2. *Для любых орф f и T существует орф $t>T$ такая, что* $R_t=R_{f(t)}$.

Из 5.2 следует

5.3. *Не существует орф s такой, что для любой орф t* $R_{s(t)}\supset R_t$.

Дальше в этом пункте мы будем интересоваться вопросами представимости классов сложности (ср.([11,12])). Пусть фиксировано

взаимнооднозначное соответствие между множеством н. ч. и б. ф. Н. ч., соответствующее б. ф. в этом соответствии будем называть ее кодом. Через $\bar{A}$ будем обозначать множество б. ф., для которого A есть множество кодов. Пусть ω_i есть множество определенности φ_i. Множество н. ч. s будем называть представлением класса R_i множеств б. ф., если $R_i = |\bar{\omega}_i| i \in s|$. Будем говорить, что класс R_i рекурсивно представим, если существует рекурсивное представление класса R_i.

5.4. *Класс R_i рекурсивно представим для любой орф t.*

Через ΩR_i будем обозначать индексное множество класса R_i, определяемое как $|i|\bar{\omega}_i \in R_i|$. Будем пользоваться обычными обозначениями „$\leqslant_T$“ и „$\leqslant_1$“ для сводимостей по Тьюрингу и 1—1 сводимости, Σ_n и Π_n для уровней иерархии Клини-Мостовского ([5]). Нам потребуются следующие „эталонные“ множества — Equal$=|\langle i, j\rangle|\varphi_i = \varphi_j|$ и Cofinite $= |i|\omega_i$ кофинитно|. Известно, что эти множества являются соответственно Π_2-полным и Σ_3-полным. Через R будем обозначать класс всех рпм н. ч.

Доказательство 5.7 следует плану доказательства аналогичного факта, формулируемого для классов сложности чрф ([12]).

5.5. (Робертсон ([12])) *Для любой орф t, если класс $R - R_t$ имеет $\Pi_3 \cap \Sigma_3$ представление, то $\Omega R_t \leqslant_T$ Equal.*

5.6. $\exists \tau \forall t > \tau |\text{Cofinite} \leqslant_1 \Omega R_t|$.

5.7. *Существует орф τ такая, что для всех $t > \tau$ неверно, что класс $R - R_t$ имеет $\Pi_3 \cap \Sigma_3$ представление.*

5.8 *Существует орф τ такая, что для всех $t > \tau$ ΩR_t Σ_3-полно.*

Пользуюсь случаем выразить благодарность И. Д. Заславскому за постоянное внимание к работе и ряд существенных замечаний.

Вычислительный центр
Министерства автомобильного транспорта
Армянской ССР

Ա. Ա. ՆԱՋԱՐՅԱՆ

Բուլյան ֆունկցիաների բազմությունների բարդության դասերի մասին

Դիտարկվում են բուլյան ֆունկցիաների բազմությունների բարդությունները բնորոշող Շենոնի ֆունկցիաներն այն պայմաններում, երբ ուսումնասիրվող ալգորիթմների աշխատանքի ժամանակը սահմանափակվում է ընդհանուր ընկուրսիվ ֆունկցիաներով։ Հաստատվում են որոշ անհրաժեշտ և բավարար պայմաններ, որպեսզի նշված Շենոնի ֆունկցիաներն ունենան հզորական գնահատականներ։ Ցույց է տրվում, որ գոյություն ունեն այնպիսի

բազմություններ, որոնց համար Ենոնի ֆունկցիաների գնահատականները էապես տարբերվում են, երբ դիտարկվում են ալգորիթմները սահմանափակումների տակ և բացակայության դեպքերում։ Դիտարկվում են բուլյան ֆունկցիաների բազմությունների բարդության դասերը և այդ դասերի դասակարգումները։

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *А. К. Звонкин, Л. А. Левин*, УМН, т. 25, вып. 2(1970), 85—127. [2] *Г. А. Назарян*, ДАН АрмССР, том V, 3 (1972), 129—133. [3] *А. Н. Колмогоров*, Проблемы передачи информации I. 1(1965). [4] *И. Д. Заславский*, Зап. научн. семинаров ЛОМИ АН СССР, т. 16, 65—76, (1969). [5] *Х. Роджерс*, Теория рекурсивных функций и эффективная вычислимость, изд. «Мир», М., 1972. [6] *Я. М. Барздинь*, ДАН СССР, 182, 1249—1255, (1968). [7] *Н. В. Петри*, Зап. научн. семинаров ЛОМИ АН СССР, т. 16, 165—174, (1969). [8] *М. И. Канович*, Исследования по теории алгоритмов и математической логике. ВЦ АН СССР, 3—42, М., 1973. [9] *М. Г. Гельфонд*, Зап. научн. семинаров ЛОМИ АН СССР, т. 16, 20—28, (1969). [10] *Д. Хартманис, Д. Э. Хопкрофт*, Киб. сборник (новая серия) вып. 11, 131—176, М., 1974. [11] *L. H. Landweber, E. L. Robertson*, JACM, v. 19, № 2, 296—309 (1972). [12] *E. L. Robertson*, JCSS, №1, 69–87, 9 (1974).