ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXI 1975 2

УДК 510 : 164

МАТЕМАТИКА

Г. А. Назарян

О сложности частотных вычислений и сложности доопределений булевых функций

(Представлено академиком АН Армянской ССР С. Н. Мергеляном 2/VI 1975)

В статье рассматриваются две взаимосвязанные задачи: а) о сложности частотных (или приближенных) вычислений булевых функций, и б) о сложности их доопределений.

1 Всюду далее орф есть сокращение для выражения «общерекурсивная функция», чрф—«частично рекурсивная функция», б.ф.—«булева функция», р. ч.—«рациональное число», н. ч.—«натуральное число». 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 как в (2). Длину н. ч. x будем обозначать через $l(x)$. Размерность б. ф. будем указывать верхним индексом: так если F есть б. ф. размерности n, то будем писать F^n наряду с F. Если A есть конечное множество н. ч., то через $d(A)$ будем обозначать мощность этого множества. Конструктивную последовательность р. ч. (ПРЧ) $\varepsilon(n)$ будем называть правильной если $\varepsilon(n) \to 0$ и $|2^n \cdot \varepsilon(n)|$ есть монотонная неограниченная последовательность н. ч. (правильной ПРЧ является, например, последовательность $2^{[\nu \cdot n]}/2^n$ где ν — р. ч. меньше единицы). Буквы T, t, f, g, ε (возможно с индексами) будем использовать для обозначения одноместных орф, h, ϖ — для двуместных орф, ε — для правильной ПРЧ, π — для ПРЧ такой, что $\pi(n) \to 0$, $\varkappa$ — для ПРЧ, ν для р. ч. меньшего единицы. C и ρ — для н. ч., наконец F, P, Q — для обозначения б. ф. Буквами r и ρ будем обозначать конструктивные функции такие, что

$$\forall n \forall F^n \forall P^n (r(F^n, P^n) = d|x|(l(x) = n) \& \overline{\ } (F^n(x) = P^n(x))|,$$
$$\rho(F^n, P^n) = r(F^n, P^n)/2^n.$$

Будем говорить, что F^n и P^n ν — равны (и писать $F^n = P^n$) если $\rho(F^n, P^n) \leqslant \nu$. Зафиксируем некоторую допустимую в смысле (3) нумерацию φ (иногда будем предполагать, что φ — аддитивно оптимальная нумерация (4, 5)). Для нумерации φ зафиксируем конструктивную последовательность Φ сигнализирующих (6). С последовательностью сигнализирующих ассоциируем последовательность чрф $\hat{\Phi}$ такую; что $\forall i \forall n (\hat{\Phi}_i(n) = \max_{l(x)=n} \Phi_i(x))$. Говорим, что чрф ψ ν — вычисля-

ет F (будем писать $\varphi^{-}\!\!\rightarrow F$), если φ вычисляет P такую, что $P = F$.

Через K будем обозначать двухместную чрф, удовлетворяющую условию $\forall n \forall C \forall F^n (K(C, F^n) = \mu p [\varphi_p \!\!\rightarrow F^n \,\&\, \Phi_p(n) < C])$. (Легко видеть, что условие $\varphi_p \!\!\rightarrow F$ алгорифмически не проверяемо, однако конъюнкция $\varphi_p \!\!\rightarrow F \,\&\, \Phi_p(n) < C$ алгорифмически проверяема). Вместо $K(C, F)$ будем в дальнейшем писать $K^C(F)$. Пусть далее K_* — чрф, удовлетворяющая условию $\forall C \forall F^n (K_*^C(F^n) = \min_{P = (n)F} K^C(P^n))$ (где $K_*^C(F)$ обозначает $K_*(C, F)$). Будем говорить, что F (p, C) вычислима (*) (соответственно (p, C) $*$ —вычислима), если $K^C(F) \leqslant p$ (если $K_*^C(F) \leqslant p$).

Конструктивную последовательность б. ф. называем правильной по Маркову (*), если при любом n n-я б. ф. этой последовательности n-местна. Записи $\forall F_n^n$ и $\exists F_n^n$ будем использовать как сокращение для высказываний „для любой конструктивной правильной последовательности б. ф.", „существует конструктивная правильная последовательность б. ф.".

Запись $a(n) = b(n)$, где a и b некоторые чрф, будет означать, что левая и правая части равенства определены и равны. Аналогично будут пониматься записи $a(n) \geqslant b(n)$ и $a(n) \leqslant b(n)$.

Мы будем употреблять обозначения вида $\forall k > m$, $\exists k > m$, $\forall T > t$, $\exists T > t$ и т. д. (где T и t — переменные для орф). Такие обозначения понимаются обычным образом, например, $\forall k > m\ R(k)$, $\exists k > m\ R(k)$, $\forall T > t R(T)$, $\exists T > t R(T)$ понимаются как $\forall k (k > m \supset R(k))$, $\exists k (k > m \,\&\, R(k))$, $\forall T (\forall n (\forall T(n) > t(n)) \supset R(T))$, $\exists T (\forall n (T(n) > t(n)) \,\&\, R(T))$. В дальнейшем рассматривая поведение произвольной сигнализирующей, мы будем иногда для краткости называть ее «время вычислений» или просто «время»; под «объемом программы p» будем понимать индекс p нумерации φ.

2. Утверждения этого пункта относятся к индивидуально рассматриваемым б. ф. они показывают, что с одной стороны переход к приближенным вычислениям б. ф. может существенно уменьшать как «объем», так и «время вычисления» б. ф. по сравнению с точными вычислениями (теорема 2,1), с другой стороны, (теорема 2,2), существуют сколь угодно сложные б. ф., сложностные характеристики которых не улучшаются при переходе от точных вычислений к приближенным.

2. 1 $\exists t \forall f \forall T \exists m \forall n > m \exists F^n \exists P^n (r(F^n, P^n) = 1 \,\&\, K^{T(n)}(F^n) \geqslant f(K^{t(n)}(P^n)))$.

Говорим, что F является $(p, C, *)$ —инициальной, если выполнены условия: а) F (p, C) вычислима, б) если F (p, C_1) $*$—вычислима, то $C_1 \geqslant C$, в) если F (p_1, C) $*$—вычислима, то $p_1 \geqslant p$. Таким образом, б. ф. является $(p, C, *)$ —инициальной, если переход к приближенным вычислениям с допустимой частотой ошибок не больше $*$ не позволяет уменьшить ни времени, ни объема вычислений.

2. 2 $\forall * \forall p \forall T \exists F^n \exists p_1 > p \exists C > T(n)$ [$F(p_1, C, *(n))$ —инициальная].

3. Нетрудно убедиться, что проблема поиска $*$ —минимальных

программ" для б. ф. (т. е. программ наименьшего объема вычисляющих данные б. ф.) неразрешимы (ср. [9]). Вместе с тем разрешима проблема поиска ε-минимальных программ вычисляющих б. ф. время ограниченное некоторой орф t от размерности б. ф. (при достаточно больших t). В последнем случае мы имеем дело с разрешением некоторой ограниченной массовой проблемы, связанной с выявлением нетривиальных функциональных свойств алгорифмов. Естественно ожидать, что (ср. [10]) время работы алгорифмов, ее разрешающих велико. Это предположение подтверждает утверждение 3. 1.

Нетрудно убедиться, что можно указать орф t, для которой выполнено $\forall n \forall F^n (\mathcal{K}^{t(n)}(F^n))$. В определении (π, T) —минимизирующей орф ниже предполагаем, что $T > t$. Орф g будем называть (π, T) минимизирующей, если $\forall n \forall F^n (g(F^n) = K^{T(n)}(F^n))$.

Символом $\mathrm{Min}(g, \pi, T)$ будем обозначать высказывание: орф g является (π, T) —минимизирующей.

3.1 $\forall \pi \exists h \forall T \forall z (\mathrm{Min}(z, \pi, T) \supset \forall_n^\infty (T(n) < h(n, \Phi_z(2^n))))$.

Таким образом время T рекурсивно ограничено временем работы (π, T) —минимизирующих алгорифмов, иначе говоря невозможно (π, T) —минимизировать со скоростью, существенно меньшей чем T.

С другой стороны, нетрудно убедиться, что если рассматривать честные ([11]) орф T, то можно строить (π, T) —минимизирующие алгорифмы, время работы которых не существенно превосходит T.

Замечание. Теорема 3.1 справедлива для произвольной ПРЧ π такой, что $\pi(n) \to 0$. При $\pi(n) < 2^{-n}$ значениями всякой (π, T) —минимизирующей орф являются программы точно вычисляющие б. ф.

3.2 $\forall \pi \forall f \forall t \exists T > t (\mathrm{Min}(g_1, \pi, T) \,\&\, \mathrm{Min}(g_2, \pi, f(T)) \supset$
$\supset \forall^\infty n \forall F^n (g_1(F^n) = g_2(F^n)))$.

Утверждение 3.2 является некоторым аналогом теоремы о пробеле ([12]). ([13]). Как следует из 3.1. время вычисления орф g_2 из утверждения 3.2 должно быть больше времени вычисления орф g_1, но g_2 минимизирует не лучше, чем g_1 (см. ниже).

Говорим, что (π, t_1) —минимизирующая орф g_1 улучшает (π, t_2) минимизирующую орф g_2, если $\exists_n^\infty (\sum_{F^n \in M^n} g_1(F^n) < \sum_{F^n \in M^n} g_2(F^n))$, где M^n — класс всех б. ф. от n аргументов. Ясно, что это возможно лишь при условии, что $\exists_n^\infty (t_1(n) > t_2(n))$. Из 3.2 легко следует

3.3 $\forall \pi \exists f \forall t (\mathrm{Min}(g_1, \pi, t) \,\&\, \mathrm{Min}(g_2, \pi, f(t)) \supset (g_2$ улучшает $g_1)$

4. Говорим, что t есть нижняя оценка (верхняя оценка) вычисления последовательности б. ф. F_n^n, если $\forall j (\forall^\infty n (\varphi_j \neq F_n^n) \supset \forall_n^\infty (\Phi_j(n) > t(n)))$ (соответственно $\exists j (\forall^\infty n (\varphi_j \neq F_n^n) \,\&\, \forall_n^\infty (\Phi_j(n) < t(n)))$.

Будем говорить, что t есть нижняя оценка a-вычисления F_n^n, если $\forall j (\forall^\infty n (\varphi_j \overset{a(n)}{\neq} F_n^n) \supset \forall_n^\infty (\Phi_j(n) > t(n)))$. Символами $V(t, F_n^n)$, $V_a(t, F_n^n$

и $U(t, F_n^n)$ будем обозначать соответственно высказывания: t есть нижняя оценка вычисления F_n^n, t есть нижняя оценка τ-вычисления F_n^n и t есть верхняя оценка вычисления F_n^n.

4.1. $\forall T \forall F_n^n \exists P_n^n (\forall n (r(F_n^n, P_n^n) \leqslant 1) \& V(T, F_n^n))$.

Факт близкий к 4.1 сформулирован в ([14]). Из 4.1 следует, что малые жертвы в точности вычислений последовательностей б. ф. могут приводить к сколь угодно большим выигрышам во времени вычислений. Следующее предложение утверждает, что существуют последовательности б. ф., составленные из индивидуально простых б. ф., но вместе с тем время их вычисления (даже приближенное) достаточно велико.

4.2. *Существуют орф t и н. ч. C такие, что для любой ПРЧ τ такой, что для всех n $\tau(n) < \frac{1}{2}$ выполнено:* $\forall T \exists F_n^n \forall_\tau (K^{T(n)}(F_n^n) < C \& V_\tau(T, F_n^n))$.

Орф t будем называть ω-честной [11], если существует н. ч. z такое, что $\varphi_z = t$ и $\forall_n^\tau (\Phi_z(n) < \omega(n, t(n)))$.

4.3 $\exists T \exists C \forall \omega \exists \omega_1 \forall (\omega\text{-честной } t) \exists F_n^n \forall_\tau \left(\tau(n) < \frac{1}{2}\right) (V_\tau(t, F_n^n) \&$ $U(\omega_1(n, t(n)), F_n^n) \& \forall n (K^{T(n)}(F_n^n) < C))$.

5. В этом пункте мы будем интересоваться вопросами доопределений частично заданных б.ф. (ч.б.ф.) Вопросы доопределений ч.б.ф связаны с вопросами приближенных вычислений б.ф. Пусть A — конечное множество пар $|<x_i, y_i>|$. Через $L(A)$ и $R(A)$ будем обозначать соответственно множество левых и правых элементов пар из A. Через N_n будем обозначать множество н. ч. длины n.

Конечное множество пар $|<x_i, y_i>|$ будем называть таблицей (*) если выполнено $x_i = x_j \supset i = j$. Под ч. б. ф. F^n будем понимать таблицу такую, что $L(F^n) \subseteq N_n$ и $R(F^n) \subseteq |0, 1|$. Будем говорить, что таблица A есть G доопределение ч. б. ф. F^n (где G — конечное множество н. ч.) если $A \supseteq F^n$ и $L(A) = N_n$ и $R(A) \subseteq G \subseteq |0, 1|$. Говорим, что таблица $A = |<x_i, y_i>|$ есть стандартное $|k|$— доопределение ч. б. ф. F^n (будем записывать $(F^n)^{|k|}$, если выполнено: $x_i \in N_n \supset L(F^n) \supset y_i = k$. Под булевским доопределением ч. б. ф. F будем понимать $|0, 1|$ доопределение F. Говорим, что ч. р. ф. ψ вычисляет ч. б. ф. F^n, если $\forall x((x \notin N_n \supset ! \psi(x)) \& (x \in L(F^n) \supset <x, \psi(x)> \in F^n)$.

Таким образом, если ψ вычисляет ч. б. ф. F, то она вычисляет некоторое G доопределение F. Простейшим способом доопределений ч. б. ф. является стандартное $|k|$-доопределение, но стандартно $|k|$-доопределяя при $k \neq 0,1$ мы фактически выделяем область определенности (либо неопределенности) ч. б. ф., а следовательно увеличиваем информативность и соответственно сложность доопределения. Поэтому более естественными представляются булевские стандартные доопределения, т. е. $k = 1$, либо $k = 0$. Утверждения 5.1—5.5 служат аргументом в пользу сказанного. В утверждениях 5.1 и 5.2 нумерации чрф φ предполагается

аддитивно оптимальной, они относятся к индивидуально рассматриваемым ч. б. ф. Утверждения 5.3—5.5 относятся к последовательностям ч. б. ф.

5.1. $\exists C \forall T \exists_i \forall_n \forall F^n (K^{T(n)}(F^n)(1) \leqslant K^{T(n)}(F^n(2)) \cdot C)$.

5.2. Существуют орф T и константы C_1, C_2 и псевдопоследовательность ((5), (15)) ч. б. ф. F^n_n такие, что $\forall n (K^{T(n)}((F^n_n)(1)) < C_1 \& (K(F^n_n)(2) > 2^{n-C_2})$.

5.3. $\exists^2 \exists f \forall F^n_n \forall_j |(\forall n (\varphi_j(n) \rightarrow (F^n_n)(2)) \supset \forall n (\varphi_{s(j)n} \rightarrow (F^n_n)(1)) \&$

$$\& \forall^{\infty}_n (\Phi_{s(j)n} < f(\hat{\Phi}_j(n)))|.$$

Через $L(F^n_n)$, где F^n_n — последовательность ч. б. ф., будем обозначать множество определенности последовательности ч. б. ф., $F^n_n - \bigcup_{n \in N} L(F^n_n)$ и через χ_L — характеристическую функцию множества L.

5.4. $\exists h \exists^2 \forall F^n_n \forall_j (\forall n (\varphi_j(n) \rightarrow (F^n_n)(2)) \supset |\varphi_{s(j)} = \chi_{L(F^n_n)}$

$$\& \forall^{\infty}_n (\Phi_{s(j)}(n) < h(n, \hat{\Phi}_j(n)))|).$$

5.5. $\exists l \forall T \exists F^n_n (V(T, (F^n_n)(2)) \& U(l, (F^n_n)(1)))$.

В дальнейшем под доопределением ч. б. ф. будем понимать булевские доопределения, т. е. G полагается равным $\{0,1\}$. Факты, сформулированные в пунктах 2—4 свидетельствуют о том, что выбор тех или иных булевских доопределений может существенно влиять на сложностные характеристики вычислений доопределений ч. б. ф. Через $L'(F^n)$ будем обозначать множество $N_n - L(F^n)$. Из 2.1 следует:

5.6. $\exists l \forall T \forall f \exists_m \forall_n > m \exists F^n (d(L'(F^n) = 1)) \exists P^n \exists Q^n$

(P^n и Q^n *суть доопределения* F^n) & $(K^{T(n)}(P^n) > f(K^{(n)}(Q^n)))$.

5.7. $\exists l \forall T \exists F^n_n (\forall n (d(L'(F^n_n)) \leqslant 1)) \exists P^n_n \exists Q^n_n$

$\forall n (P^n_n$ и Q^n_n *суть доопределения* F^n_n) & $V(T, P^n_n)$ & $U(l, F^n_n)$.

Говорим, что б. ф. F^n есть наилучшее C доопределение ч. б. ф. P^n, если для любого доопределения ч. б. ф. Q^n выполнено $K^C(F^n) \leqslant K^C(Q^n)$. Геделев номер ч. б. ф. F будем обозначать посредством $\bar{F}$. Множество геделевых номеров ч. б. ф. F размерности n будем обозначать посредством $\mathrm{Ged}(n)$. Пусть далее Φ_l есть последовательность чрф, удовлетворяющая условию $\forall i \forall n (\Phi_l(n) = \max_{x \in \mathrm{Ged}(n)} \Phi_l(x))$.

Нетрудно убедиться, что для любой l (достаточно большой) существует орф g (ее мы будем называть l-доопределяющей) такая, что для любого n, для любой ч. б. ф. F^n, б. ф., вычисляемая чрф $?_{g(\bar{F}^n)}$ есть наилучшее $l(n)$ доопределение F^n. Естественно ожидать, что время работы l-доопределяющих алгорифмов так же как и минимизирующих не будет существенно меньшим, чем l. Рекурсивность

(ε, t)-минимизирующих алгорифмов (при фиксированном ε) относительно t-доопределяющих позволяет легко из 3.1 получить

5.8. $\exists t \exists h \forall T > t \forall z((z\ t\text{-доопределяет}) \supset \forall_n^{\infty}(T(n) < h(n, \Phi_z(n)))$.

Очевидно следующее утверждение

5.9. *Если б. ф. $F^n(p, C, \nu)$ — инициальна, то F есть наилучшее C доопределение для множества ч. б. ф. P^n таких, что $d(L'(P^n)) < |\nu \cdot 2^n|$ и F^n есть доопределение P^n.*

Пользуюсь случаем выразить глубокую благодарность Н. Д. Заславскому, под руководством которого выполнена настоящая работа.

Вычислительный центр МАТ Армянской ССР

Հ. Հ. ՆԱԶԱՐՅԱՆ

Բուլյան ֆունկցիաների մոտավոր հաշվման և շարունակման բարդության մասին

Դիտարկվում է Բուլյան ֆունկցիաների (բ. ֆ.) մոտավոր հաշվման բարդություններ։ Ցույց է տրվում, որ գոյություն ունեն ինչպես, այնպիսի բ. ֆ., որոնց մոտավոր հաշվումները թույլ են տալիս գգալիորեն պակասեցնել հաշվումների ժամանակը և ծավալը, այնպես էլ ցանկալի աստիճանի բարդ բ. ֆ., որոնց համար մոտավոր հաշվումներին անցումը (թույլատրելի մոտավորության աստիճանով) չի պակասեցնում հաշվումների ոչ ժամանակը և ոչ էլ ծավալը։ Համանման փաստեր հաստատվում են բ. ֆ. շարունակման բարդությունների համար։ Ցույց է տրվում նաև, որ նվազեցնող և շարունակող ալգորիթմների աշխատանքի ժամանակը, որոնք կառուցում են բավականին արագ աշխատող ծրագրեր, համեմատելի է այդ ծրագրերի աշխատանքի ժամանակի հետ։

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *К. Зюпкин, Л. А. Левин*, УМН, т. 25, вып. 2, 85—127 (1970). [2] *Г. А. Назарян*, ДАН Арм. ССР, т. LV, № 3 (1972), 129—133. [3] *Х. Роджерс*, Теория рекурсивных функций и эффективная вычислимость, М., «Мир», 1972. [4] *А. Н. Колмогоров*, Три подхода к определению понятия «количество информации», Проблемы передачи информации 1, 1, 3—7 (1965). [5] *Н. Д. Заславский*, О псевдофункциях Шеннона, Зап. научн. семинаров ЛОМИ АН СССР, т. 16, (1969), 65—76. [6] *M. A. Blum*, A machine—independent theory of complexity of recursive functions, IACM, 14, 322—336 (1967). [7] *М. И. Канович, И. В. Петри*, ДАН, 184, 6, 1275—1276 (1969). [8] *А. А. Марков*, Известия АН, сер. матем. 31, 161—208 (1967). [9] *D. Pager*, On the problem of finding minimal programs for tables, Information and Control, 14, 6, 550—554 (1969). [10] *Я. Я. Бичевский*, Латв. матем. ежегодник, 13, Рига, (1973). [11] *J. Hartmanis, J. Hopcroft*, IACM, 18, 3 444—475 (1971). [12] *Б. А. Трахтенброт*, Сложность алгорифмов и вычислений, Новосибирск, (1967). [13] *A. Borodin*, IACM, 19, 158—171, (1972). [14] *Б. А. Трахтенброт*, Алгебра и логика, 4, вып. 5 (1965). [15] *М. Г. Гельфонд*, Зап. научн. семинаров ЛОМИ АН СССР, т. 16, 20—28, (1969).