ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXXX 1985 4

УДК 519.95

МАТЕМАТИКА

В. А. Варданян

О сложности динамических тестов для монотонных булевых функций

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 24/XI 1983)

Введем следующие обозначения: B^n—множество наборов n-мерного единичного куба; $P_2(n)$ (соответственно $P_2^c(n)$)—множество всех булевых функций, (существенно) зависящих от переменных $x_1, x_2, \ldots, x_n$; $M(n)$—множество всех монотонных функций $f \in P_2(n)$; $M^c(n) = M(n) \cap P_2^c(n)$; $\leqslant^*$—отношение предшествования в B^n; $|A|$—число элементов множества A; $[x](]x[)$—наибольшее (наименьшее) целое, не превосходящее (не меньшее) x. Пусть $\bar{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in B^n$, обозначим $\bar{\alpha}^i = (\alpha_1, \ldots, \alpha_{i-1}, \bar{\alpha}_i, \alpha_{i+1}, \ldots, \alpha_n)$, $1 \leqslant i \leqslant n$; $B^{n,k} = \{\bar{\alpha} \in B^n / \sum_{i=1}^{n} \alpha_i = k\}$, $0 \leqslant k \leqslant n$; $N(\bar{\alpha}) = \{i / \alpha_i = 1,\ 1 \leqslant i \leqslant n\}$; $N_r(\bar{\alpha}) = N(\bar{\alpha}) \setminus \{r\}$, $1 \leqslant r \leqslant n$.

Будем говорить, что функция $f \in P_2(n)$ активна на наборе $\bar{\alpha}$ по направлению i, $1 \leqslant i \leqslant n$, если $f(\bar{\alpha}) \neq f(\bar{\alpha}^i)$. Функция f называется активной по направлению i, если существует набор $\bar{\alpha} \in B^n$ такой, что $f(\bar{\alpha}) \neq f(\bar{\alpha}^i)$.

Активностью функции f на наборе $\bar{\alpha}$ назовем число $\omega^f(\bar{\alpha}) = \sum_{i=1}^{n} (f(\bar{\alpha}) \oplus f(\bar{\alpha}^i))$. Число $\omega^f = \max_{\bar{\alpha} \in B^n} \omega^f(\bar{\alpha})$ называется [1] активностью функции f.

Множество наборов $T(f) \subseteq B^n$ называется (единичным) динамическим тестом [1] для функции f, если для каждого i, $1 \leqslant i \leqslant n$, из активности функции f по направлению i следует существование набора $\bar{\alpha} \in T(f)$ такого, что $f(\bar{\alpha}) \neq f(\bar{\alpha}^i)$. Тест $T(f)$ называется минимальным, если содержит минимальное число наборов среди всех динамических тестов функции f.

Лемма 1. *Пусть* $\bar{\alpha} \leqslant^* \bar{\beta}$, $f \in M(n)$. *Тогда если* $f(\bar{\alpha}) = f(\bar{\beta}) = 0$, то $\omega^f(\bar{\alpha}) \leqslant \omega^f(\bar{\beta})$, *если же* $f(\bar{\alpha}) = f(\bar{\beta}) = 1$, *то* $\omega^f(\bar{\alpha}) \geqslant \omega^f(\bar{\beta})$.

Лемма 2. *Если* $f \in M(n)$, *то* $\omega^f = \max_{\bar{\alpha} \in \mathfrak{M}(f)} \omega^f(\bar{\alpha})$, *где* $\mathfrak{M}(f)$—*множество верхних нулей и нижних единиц функции* f.

Теорема 1. *Для почти всех функций* $f \in M(n)$ *имеет место*

$$\omega^f = \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

Пусть $\omega_M(n)=\min\limits_{f\in M^c(n)}\omega^f$.

Теорема 2. $\omega_M(n)\leqslant\frac{1}{2}\log_2 n$ *при* $n\to\infty$.

Доказательство. Пусть $\varphi(n)$—положительная целочисленная функция, удовлетворяющая условию $C_{\varphi(n)}^{\left[\frac{1}{2}\varphi(n)\right]}\geqslant n-\varphi(n)\geqslant 0$. Рассмотрим множество $I_{\varphi(n)}=\{1, 2, \ldots, \varphi(n)\}$. Через $\mathcal{N}(I_{\varphi(n)})$ обозначим множество всех $\left(\varphi(n), \left[\frac{1}{2}\varphi(n)\right]\right)$-сочетаний из множества $I_{\varphi(n)}$. Пусть ν—некоторое инъективное отображение множества $\bar{I}_{\varphi(n)}=\{\varphi(n)+1, \varphi(n)+2, \ldots, n\}$ в множество $\mathcal{N}(I_{\varphi(n)})$:

$$\nu(s)=\{\nu_1(s), \nu_2(s), \ldots, \nu_{\left[\frac{1}{2}\varphi(n)\right]}(s)\}\in\mathcal{N}(I_{\varphi(n)}),\ s\in\bar{I}_{\varphi(n)}.$$

Рассмотрим функцию $f_{\varphi(n),\nu}(x_1, x_2, \ldots, x_n)=\bigvee\limits_{1\leqslant i_1<i_2<\ldots<i_{\left[\frac{1}{2}\varphi(n)\right]+1}\leqslant\varphi(n)}\times$

$\times x_{i_1}x_{i_2}\ldots x_{i_{\left[\frac{1}{2}\varphi(n)\right]+1}}\bigvee\limits_{\varphi(n)+1\leqslant s\leqslant n} x_s x_{\nu_1(s)}x_{\nu_2(s)}\ldots x_{\nu_{\left[\frac{1}{2}\varphi(n)\right]}(s)}$.

Очевидно, что $f_{\varphi(n),\nu}\in M^c(n)$. Докажем, что

$$\omega^{f_{\varphi(n),\nu}}=\left[\frac{1}{2}\varphi(n)\right]+1.$$

Для любого s, $\varphi(n)+1\leqslant s\leqslant n$, рассмотрим набор $\tilde{\alpha}\in B^n$, для которого $N(\tilde{\alpha})=\{\nu_1(s), \nu_2(s), \ldots, \nu_{\left[\frac{1}{2}\varphi(n)\right]}(s)\}$. Из определения функции $f_{\varphi(n),\nu}$ следует, что $f_{\varphi(n),\nu}(\tilde{\alpha})=0$ и

$$f_{\varphi(n),\nu}(\tilde{\alpha}^i)=\begin{cases}1, & \text{если } i\in(I_{\varphi(n)}\setminus N(\tilde{\alpha}))\cup\{s\}.\\ 0, & \text{в противном случае.}\end{cases}$$

Следовательно, $\omega^{f_{\varphi(n),\nu}}(\tilde{\alpha})=|(I_{\varphi(n)}\setminus N(\tilde{\alpha}))\cup\{s\}|=\left[\frac{1}{2}\varphi(n)\right]+1$.

Теперь покажем, что не существует набора $\tilde{\alpha}\in B^n$, для которого $\omega^{f_{\varphi(n),\nu}}(\tilde{\alpha})\geqslant\left[\frac{1}{2}\varphi(n)\right]+2$. Предположим обратное: пусть $\tilde{\alpha}\in B^n$ и $\omega^{f_{\varphi(n),\nu}}(\tilde{\alpha})\geqslant\left[\frac{1}{2}\varphi(n)\right]+2$. Если $f_{\varphi(n),\nu}(\tilde{\alpha})=1$, то из монотонности функции $f_{\varphi(n),\nu}$ вытекает существование набора $\tilde{\beta}\in B^n$, $\tilde{\beta}\leqslant^*\tilde{\alpha}$, являющегося нижней единицей для $f_{\varphi(n),\nu}$, и согласно лемме 1 $\omega^{f_{\varphi(n),\nu}}(\tilde{\beta})\geqslant\omega^{f_{\varphi(n),\nu}}(\tilde{\alpha})\geqslant$ $\geqslant\left[\frac{1}{2}\varphi(n)\right]+2$. Но эти неравенства означают, что набор $\tilde{\beta}$ расположен не ниже слоя $B^{n,\left[\frac{1}{2}\varphi(n)\right]+2}$. Очевидно, последнее является противоречием, т. к. по определению все нижние единицы функции $f_{\varphi(n),\nu}$ находятся на слое $B^{n,\left[\frac{1}{2}\varphi(n)\right]+1}$.

Пусть теперь $f_{\varphi(n),\nu}(\tilde{\alpha})=0$. Рассмотрим все допустимые случаи и покажем, что они противоречат определению функции $f_{\varphi(n),\nu}$.

Случай 1. $\alpha_s=\alpha_m=0$, $f_{\varphi(n),\nu}(\tilde{\alpha}^s)=f_{\varphi(n),\nu}(\tilde{\alpha}^m)=1$, $s\neq m$, $s, m\in\bar{I}_{\varphi(n)}$.

Очевидно, существуют наборы $\bar{\beta}$ и $\bar{\gamma}$, $\bar{\beta}\leqslant^{*}\bar{\alpha}^{s}$, $\bar{\gamma}\leqslant^{*}\bar{\alpha}^{m}$, являющиеся нижними единицами для функции $f_{\varphi(n),\nu}$. Легко заметить, что $N_s(\bar{\beta})\subseteq N(\bar{\alpha})$, $N_m(\bar{\gamma})\subseteq N(\bar{\alpha})$. Из определения функции $f_{\varphi(n),\nu}$ вытекает, что $N_s(\bar{\beta})\subset I_{\varphi(n)}$, $N_m(\bar{\gamma})\subset I_{\varphi(n)}$; $|N_s(\bar{\beta})|=|N_m(\bar{\gamma})|=\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor$. Рассмотрим множество $N_s(\bar{\beta})\cup N_m(\bar{\gamma})\subseteq N(\bar{\alpha})$. Если $|N_s(\bar{\beta})\cup N_m(\bar{\gamma})|=\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor$, т. е. $N_s(\bar{\beta})=N_m(\bar{\gamma})=\{j_1, j_2, \ldots, j_{\left[\frac{1}{2}\varphi(n)\right]}\}$, то получаем, что элементарные конъюнкции $x_{j_1}x_{j_2}\ldots x_{j_{\left[\frac{1}{2}\varphi(n)\right]}}x_s$ и $x_{j_1}x_{j_2}\ldots x_{j_{\left[\frac{1}{2}\varphi(n)\right]}}x_m$ входят в сокращенную днф функции $f_{\varphi(n),\nu}$, но, очевидно, это противоречит определению функции $f_{\varphi(n),\nu}$. Если же $|N_s(\bar{\beta})\cup N_m(\bar{\gamma})|\geqslant\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor+1$, то найдется множество индексов

$$\{j_1, j_2, \ldots, j_{\left[\frac{1}{2}\varphi(n)\right]+1}\}\subseteq N_s(\bar{\beta})\cup N_m(\bar{\gamma})\subseteq N(\bar{\alpha})\cap I_{\varphi(n)}$$

такое, что элементарная конъюнкция $x_{j_1}x_{j_2}\ldots x_{j_{\left[\frac{1}{2}\varphi(n)\right]+1}}$ входит в сокращенную днф функции $f_{\varphi(n),\nu}$. Тогда из монотонности функции $f_{\varphi(n),\nu}$ следует, что $f_{\varphi(n),\nu}(\bar{\alpha})=1$. Однако последнее противоречит условию $f_{\varphi(n),\nu}(\bar{\alpha})=0$.

Случай 2. $\alpha_s=0$, $\alpha_{t_j}=0$, $f_{\varphi(n),\nu}(\bar{\alpha}^{s})=f_{\varphi(n),\nu}(\bar{\alpha}^{t_j})=1$,

$$s\in\overline{I}_{\varphi(n)},\ t_j\in I_{\varphi(n)},\ 1\leqslant j\leqslant\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor+1.$$

Пусть $\bar{\beta}\leqslant^{*}\bar{\alpha}^{s}$ и $\bar{\beta}$—нижняя единица для функции $f_{\varphi(n),\nu}$. Легко видеть, что $N_s(\bar{\beta})\subseteq N(\bar{\alpha})$, $N_s(\bar{\beta})\subseteq I_{\varphi(n)}$, $|N_s(\bar{\beta})|=\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor$. Следовательно, $N_s(\bar{\beta})\subseteq N(\bar{\alpha})\cap I_{\varphi(n)}$. Очевидно, что $t_j\notin N(\bar{\alpha})$, $1\leqslant j\leqslant\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor+1$. Следовательно, $|N(\bar{\alpha})\cap I_{\varphi(n)}|\leqslant\varphi(n)-\left(\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor+1\right)=\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor-1$. Таким образом, приходим к противоречию $\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor=|N_s(\bar{\beta})|\leqslant|N(\bar{\alpha})\cap I_{\varphi(n)}|\leqslant\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor-1$.

Случай 3. $\alpha_{t_j}=0$. $f_{\varphi(n),\nu}(\bar{\alpha}^{t_j})=1$, $t_j\in I_{\varphi(n)}$, $1\leqslant j\leqslant r$, $r\geqslant\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor+2$.

Рассмотрим набор $\bar{\alpha}^{t_1}$. Существует набор $\bar{\beta}$, $\bar{\beta}\leqslant^{*}\bar{\alpha}^{t_1}$, являющийся нижней единицей для функции $f_{\varphi(n),\nu}$. Очевидно, что $N_{t_1}(\bar{\beta})\subseteq N(\bar{\alpha})$, $N_{t_1}(\bar{\beta})\cap I_{\varphi(n)}\subseteq N(\bar{\alpha})\cap I_{\varphi(n)}$, $t_j\notin N(\bar{\alpha})$, $1\leqslant j\leqslant r$. Из определения функции $f_{\varphi(n),\nu}$ имеем $\left\lfloor\frac{1}{2}\varphi(n)\right\rfloor-1\leqslant|N_{t_1}(\bar{\beta})\cap I_{\varphi(n)}|$. Таким образом, опять при-

ходим к противоречию $\left[\frac{1}{2}\varphi(n)\right]-1\leqslant|N_{t_1}(\bar{\beta})\cap I_{\varphi(n)}|\leqslant|N(\bar{\alpha})\cap I_{\varphi(n)}|\leqslant$

$\leqslant\varphi(n)-r\leqslant\varphi(n)-\left(\left|\frac{1}{2}\varphi(n)\right|+2\right)=\left|\frac{1}{2}\varphi(n)\right|-2.$

Итак, полученные противоречия доказывают справедливость равенства $\omega^{f_{\varphi(n),\nu}}=\left|\frac{1}{2}\varphi(n)\right|+1$.

Теперь нетрудно проверить, что при больших n и $\varphi(n)$, где

$\varphi(n)=\left|\log_2 n+\frac{1}{2}\log_2\log_2 n+\eta(n)\right|$, $\eta(n)\to\infty$, $\eta(n)=o(\log_2\log_2 n)$, $n\to\infty$,

справедливо неравенство $C^{\left|\frac{1}{2}\varphi(n)\right|}_{\varphi(n)}>n-\varphi(n)>0$. Следовательно,

$$\omega_M(n)\leqslant\omega^{f_{\varphi(n),\nu}}=\left|\frac{1}{2}\varphi(n)\right|+1=\frac{1}{2}\log_2 n\left(1+O\left(\frac{\log_2\log_2 n}{\log_2 n}\right)\right).$$

Теорема доказана.

Следствие. Пусть $\omega(n)=\min\limits_{f\in P_2^c(n)}\omega^f$. Тогда $\omega(n)\lesssim\frac{1}{2}\log_2 n$ при $n\to\infty$.

Пусть $T(f)$ — минимальный динамический тест для f.

Теорема 3. *Для почти всех функций* $f\in M(n)$ $|T(f)|=2$.

Рассмотрим функцию Шеннона $T_M(n)=\max\limits_{f\in M^c(n)}|T(f)|$.

Теорема 4. *При больших* n *справедливы неравенства*

$$n-\log_2 n-O(\log_2\log_2 n)\leqslant T_M(n)\leqslant n-\log_2 n+O\left(\frac{\log_2 n}{n}\right).$$

Доказательство. *Верхняя оценка.* Из (3) следует, что для любой функции $f\in P_2(n)$ при $n\geqslant 1$ имеет место $|T(f)|\leqslant n-t$, где t определяется из $2^{t-1}+t\leqslant n\leqslant 2^t+t$, откуда получаем, что при больших n

$$T_M(n)\leqslant n-\log_2 n+O\left(\frac{\log_2 n}{n}\right).$$

Нижняя оценка. Рассмотрим функцию $f_{\varphi(n),\nu}$, определенную при доказательстве теоремы 2, где $\varphi(n)=\left|\log_2 n+\frac{1}{2}\log_2\log_2 n+\eta(n)\right|$, $\eta(n)=o(\log_2\log_2 n)$, $\eta(n)\to\infty$, $n\to\infty$. Покажем, что для любых s, $m\in\overline{I}_{\varphi(n)}$, $s\neq m$ не существует набора $\bar{\alpha}\in B^n$ такого, что

$$f_{\varphi(n),\nu}(\bar{\alpha})\neq f_{\varphi(n),\nu}(\bar{\alpha}^s),\quad f_{\varphi(n),\nu}(\bar{\alpha})\neq f_{\varphi(n),\nu}(\bar{\alpha}^m).$$

Предположим обратное: пусть существует набор $\bar{\alpha}\in B^n$ такой, что последние неравенства справедливы. Поскольку $f_{\varphi(n),\nu}\in M(n)$, то возможны два случая. Мы докажем, что они оба противоречат определению функции $f_{\varphi(n),\nu}$.

Случай 1. $f_{\varphi(n),\nu}(\bar{\alpha})=1$, $\alpha_s=\alpha_m=1$, $f_{\varphi(n),\nu}(\bar{\alpha}^s)=f_{\varphi(n),\nu}(\bar{\alpha}^m)=0$. Очевидно, существует набор $\bar{\beta}\in B^n$, $\bar{\beta}\leqslant^*\bar{\alpha}$, являющийся нижней единицей для $f_{\varphi(n),\nu}$, $\beta_s=\beta_m=1$, $f_{\varphi(n),\nu}(\bar{\beta}^s)=f_{\varphi(n),\nu}(\bar{\beta}^m)=0$. Тогда нетрудно заметить,

что в сокращенной днф функции $f_{\varphi(n),\nu}$ должна существовать элементарная конъюнкция, содержащая переменные x_s и x_m, но это противоречит определению функции $f_{\varphi(n),\nu}$.

Случай 2. $f_{\varphi(n),\nu}(\tilde{\alpha})=0$, $\alpha_s=\alpha_m=0$, $f_{\varphi(n),\nu}(\tilde{\alpha}^s)=f_{\varphi(n),\nu}(\tilde{\alpha}^m)=1$. Противоречивость этого случая была показана при доказательстве теоремы 2 (случай 1). Следовательно, любой динамический тест функции $f_{\varphi(n),\nu}$ содержит не менее $n-\varphi(n)$ наборов. Таким образом, $|T(f_{\varphi(n),\nu})|\geqslant n-\varphi(n)=n-\log_2 n-O(\log_2\log_2 n)$ при больших n. Следовательно, $T_M(n)\geqslant n-\log_2 n-O(\log_2\log_2 n)$. Теорема доказана.

Вычислительный центр Академии наук
Армянской ССР и Ереванского
государственного университета

Վ. Ա. ՎԱՐԴԱՆՅԱՆ

Մոնոտոն բուլյան ֆունկցիաների դինամիկ տեստերի բարդության մասին

Ապացուցված են հետևյալ պնդումները.

1. Համարյա բոլոր $f\in M(n)$ մոնոտոն բուլյան ֆունկցիաների համար $\omega^f=]n/2[+1$, որտեղ ω^f-ը f ֆունկցիայի ակտիվությունն է, n-ը՝ փոփոխականների քանակը։

2. $\omega_M(n)=\min\limits_{f\in M^c(n)}\omega^f\leqslant\frac{1}{2}\log_2 n$ երբ $n\to\infty$, որտեղ $M^c(n)$-ը այն մոնոտոն ֆունկցիաների բազմությունն է, որոնք էապես են կախված բոլոր n փոփոխականներից։

3. Համարյա բոլոր $f\in M(n)$ մոնոտոն ֆունկցիաների համար $|T(f)|=2$, որտեղ $|T(f)|$-ը f ֆունկցիայի դինամիկ տեստի բարդությունն է։

4. $T_M(n)=\max\limits_{f\in M^c(n)}|T(f)|\sim n$ երբ $n\to\infty$.

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *А. В. Петросян*, Tanulmányok, Будапешт, № 135 (1982). [2] *Г. Р. Погосян*, О проверяющих тестах для логических схем, ВЦ АН СССР, М., 1982.