ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXXVII 1983 3

УДК 519.95

МАТЕМАТИКА

В. А. Варданян

О сложности динамических тестов для булевых функций

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 15/II 1983)

Понятие «динамического теста» предложено А. В. Петросяном в работе ([1]), где изучены единичные динамические тесты для классов линейных, монотонных и симметрических булевых функций. В настоящей работе приведены асимптотические оценки сложности минимального динамического теста для почти всех булевых функций. Эти оценки получены на основе вероятностных методов ([2,3,4]).

Введем следующие обозначения: B^n—множество наборов n-мерного единичного куба; $P_2(n)$—множество всех булевых функций, зависящих от n переменных; $|A|$—число элементов множества A; $H(p)=-p\log p-(1-p)\log(1-p)$, $0<p<1$, где символ log означает логарифм по основанию 2.

Пусть $\tilde{\alpha}=(\alpha_1, \alpha_2, \ldots, \alpha_n)\in B^n$, $I=\{i_1, i_2 \ldots, i_k\}\subseteq\{1, 2, \ldots, n\}$, положим $(\tilde{\alpha})^I=(\alpha_1, \ldots, \alpha_{i_1-1}, \overline{\alpha_{i_1}}, \alpha_{i_1+1}, \ldots, \alpha_{i_k-1}, \overline{\alpha_{i_k}}, \alpha_{i_k+1}, \ldots \alpha_n)$.

Определение 1 ([1]). Функция $P_2(n)$ называется активной по совокупности направлений $I\subseteq\{1, 2, \ldots, n\}$, $I\neq\varnothing$, если существует набор $\tilde{\alpha}\in B^n$ такой, что $f(\tilde{\alpha})\neq f((\tilde{\alpha})^I)$.

Определение 2. Функция $f\in P_2(n)$ называется активной, если она активна по каждой совокупности направлений $I\subseteq\{1, 2, \ldots, n\}$, $I\neq\varnothing$.

Через A_n обозначим множество всех активных функций $f\in P_2(n)$.

Определение 3 ([1]). Активностью функции $f\in P_2(n)$ на наборе $\tilde{\alpha}\in B^n$ называется величина $\omega^f(\alpha)=\sum_{i=1}^{n}[f(\tilde{\alpha})\oplus f((\tilde{\alpha})_i)]$. Число $\omega^f=\max_{\tilde{\alpha}\in B^n}\omega^f(\tilde{\alpha})$ называется активностью функции f, а набор $\tilde{\alpha}\in B^n$—набором активности k для функции f, если $\omega^f(\tilde{\alpha})=k$ $(0\leqslant k\leqslant n)$.

Через $\omega(k, f)$ обозначим число наборов активности k для функции $f\in P_2(n)$. Средним значением параметра $\omega(k, f)$ называется

$$\overline{\omega(k, n)}=\frac{1}{|P_2(n)|}\sum_{f\in P_2(n)}\omega(k, f).$$

Определение 4. Множество наборов $T_k(f)\subseteq B^n$ называется k-динамическим тестом для функции $f\in P_2(n)$, если для каждого подмножества $I\subseteq\{1, 2, \ldots, n\}$, $1\leqslant|I|\leqslant k$, из активности функции f по совокупности направлений I следует существование набора $\tilde{\alpha}\in T_k(f)$

такого, что $f(\tilde{\alpha})\neq f((\tilde{\alpha})^l)$. Тест $T_k(f)$ называется минимальным, если содержит минимальное число наборов среди всех k-динамических тестов для функции f.

Множество $T_1(f)$ назовем единичным динамическим тестом, а $T_n(f)$ — полным динамическим тестом для функции $f\in P_2(n)$.

Лемма 1. $\overline{\omega(k, n)}=C_n^k$, $0\leqslant k\leqslant n$.

Будем считать множество $P_2(n)$ пространством событий, в котором каждое событие $f\in P_2(n)$ происходит с вероятностью 2^{-2^n}. Определим случайную величину ξ_{nk}, принимающую значение r, $0\leqslant r\leqslant 2^n$, с вероятностью $p(n, k, r)\cdot 2^{-2^n}$, где $p(n, k, r)$ — число функций $f\in P_2(n)$, имеющих точно r наборов активности k. Очевидно, что $M\xi_{nk}=\overline{\omega(k,n)}$, где $M\xi_{nk}$ — математическое ожидание случайной величины ξ_{nk}.

Пусть $D\xi_{nk}$ — дисперсия случайной величины ξ_{nk}.

Лемма 2. $D\xi_{nk}=C_n^k+n2^{-n+1}[(C_{n-1}^{k-1})^2+(C_{n-1}^k)^2]+n(n-1)2^{-n}[(C_{n-2}^k+C_{n-2}^{k-2})^2+4(C_{n-2}^{k-1})^2]-(C_n^k)^2\cdot 2^{-n-1}(n^2+n+2)$, где $0\leqslant k\leqslant n$, $C_m^s=0$, *если* $s<0$ *или* $s>m$.

Лемма 3. *Для почти всех функций* $f\in P_2(n)$ $\omega(k, f)\sim C_n^k$ *при* $n\to\infty$, $1\leqslant k\leqslant n-1$.

Теорема 1. *Для почти всех функций* $f\in P_2(n)$ $n-1\leqslant\omega^f\leqslant n$.

Теорема 2. *Для почти всех функций* $f\in P_2(n)$, *существенно зависящих от* n *переменных, минимальный единичный динамический тест состоит не более чем из двух наборов.*

В работе [1] было показано, что доля функций $f\in P_2(n)$, минимальный единичный динамический тест для которых состоит из одного набора, стремится к $1-e^{-1}$ при $n\to\infty$. Учитывая теорему 2, получаем следующее утверждение.

Следствие. Доля функций $f\in P_2(n)$, минимальный единичный динамический тест для которых состоит из двух наборов, стремится к e^{-1} при $n\to\infty$.

Лемма 4. *Пусть множество* $Q_{skn}\subseteq B^n$ *является кодом в* B^n *с кодовым расстоянием* $2k+1$ [5] *и* $|Q_{skn}|=s$, *где* $s=[\log\sum_{l=1}^{k}C_n^l]+\varphi(n)$, $\varphi(n)$ — *целочисленная функция,* $\varphi(n)\to\infty$ *при* $n\to\infty$. *Тогда для почти всех функций* $f\in P_2(n)$ *множество* Q_{skn} *является* k-*динамическим тестом.*

Пусть $T_k(f)$ — минимальный k-динамический тест для функции $f\in P_2(n)$.

Теорема 3. 1) *При* $k=o(n)$, $n\to\infty$ *для почти всех функций* $f\in P_2(n)$

$$|T_k(f)|\leqslant k\log\frac{n}{k}.$$

2) *При* $k=[\lambda n]$, $0<\lambda<\frac{1}{4}$, $n\to\infty$ *для почти всех функций* $f\in P_2(n)$

$$|T_k(f)|\lesssim nH(\lambda).$$

Лемма 5. *Почти все функции* $f\in P_2(n)$ *активны.*

Лемма 6 (*В. Н. Носков* [4]). *Для всякого множества* $M \subseteq B^n$, $|M| = m$, *существует класс параллельных, непересекающихся* $(n-m+1)$-*мерных подкубов мощности* 2^{m-1}, *каждый подкуб из которого содержит не более одного набора из* M.

Теорема 4. 1) *При* $k = o(n)$, $k \to \infty$, $n \to \infty$ *для почти всех функций* $f \in P_2(n)$

$$|T_k(f)| \gtrsim k \log \frac{n}{k}$$

2) *При* $k = \text{const} \geqslant 2$, $n \to \infty$ *для почти всех функций* $f \in P_2(n)$

$$|T_k(f)| \gtrsim (k-1) \log n.$$

3) *При* $k = [\lambda n]$, $0 < \lambda < \frac{1}{2}$, $n \to \infty$ *для почти всех функций* $f \in P_2(n)$

$$|T_k(f)| \gtrsim \frac{nH(\lambda)}{1+H(\lambda)}.$$

4) *При* $k \geqslant n/2$, $n \to \infty$ *для почти всех функций* $f \in P_2(n)$

$$|T_k(f)| \gtrsim \frac{n}{2}.$$

Из теорем 3 и 4 вытекают следующие утверждения.

Следствие 1. *При* $k = o(n)$, $k \to \infty$, $n \to \infty$ *для почти всех функций* $f \in P_2(n)$

$$|T_k(f)| \sim k \log \frac{n}{k}.$$

Следствие 2. *При* $k = \text{const} \geqslant 2$, $n \to \infty$ *для почти всех функций* $f \in P_2(n)$

$$(k-1) \log n \lesssim |T_k(f)| \leqslant k \log n.$$

Следствие 3. *При* $k = [\lambda n]$, $0 < \lambda < 1/4$, $n \to \infty$ *для почти всех функций* $f \in P_2(n)$

$$\frac{nH(\lambda)}{1+H(\lambda)} \lesssim |T_k(f)| \leqslant nH(\lambda).$$

А. В. Петросяном и автором в неопубликованной совместной работе доказано, что для всякой функции $f \in P_2(n)$ $|T_n(f)| \leqslant n$. Учитывая четвертое утверждение теоремы 4, получаем следующее утверждение.

Следствие 4. *При* $n \to \infty$ *для почти всех функций* $f \in P_2(n)$

$$\frac{n}{2} \lesssim |T_n(f)| \leqslant n.$$

Автор выражает глубокую благодарность А. В. Петросяну и Л. А. Асланяну за ряд полезных советов.

Вычислительный центр
Академии наук Армянской ССР
и Ереванского государственного университета

Վ. Ա. ՎԱՐԴԱՆՅԱՆ

Բուլյան ֆունկցիաների դինամիկ տեստերի բարդության մասին

Աշխատանքում ներկայացված են մինիմալ k—դինամիկ տեստերի բարդության որոշ ասիմպտոտիկ գնահատականներ համարյա բոլոր բուլյան ֆունկցիաների համար։ Մասնավորապես, նշված է, որ համարյա բոլոր բուլյան ֆունկցիաների համար $n-1 \leqslant \omega^f \leqslant n$, $1 \leqslant |T_1(f)| \leqslant 2$, որտեղ ω^f-ը և $|T_1(f)|$-ը համապատասխանաբար հանդիսանում են f ֆունկցիայի ակտիվության և մինիմալ միավոր դինամիկ տեստի բարդությունը։

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *А. В. Петросян,* Tanulmányok, Будапешт, № 135 (1982). [2] *В. В. Глаголев,* Проблемы кибернетики, вып. 19 (1967). [3] *И. А. Акопова, Л. А. Асланян,* Уч. зап. ЕГУ. Естественные науки, № 1 (1980). [4] *В. Н. Носков,* Дискретный анализ, Новосибирск, вып. 27 (1975). [5] *В. И. Левенштейн,* Дискретная математика и мат. вопросы кибернетики, М., Наука, т. I (1974).