

Г.В. Антюфеев¹, Д.С. Романов²

О ТЕСТАХ ПРИ КОНСТАНТНЫХ И СДВИГОВЫХ НЕИСПРАВНОСТЯХ НА ВХОДАХ СХЕМ*

Введение

Пусть $f(x_1, x_2, \dots, x_n)$ – булева функция, зависящая от переменных x_1, x_2, \dots, x_n (это будет записываться так: $f(\tilde{x}^n) \in P_2^n$), E_2^k – множество всех k -разрядных двоичных наборов. Пусть на f действует источник U неисправностей аргументов функций (или, что тоже самое, источник U неисправностей на входах схем). Множество T наборов значений переменных x_1, x_2, \dots, x_n называется *проверяющим (соответственно, диагностическим) тестом относительно источника неисправностей U , действующего на функцию f* , тогда и только тогда, когда для любой функции $g(\tilde{x}^n)$, порождённой источником U , такой, что $g(\tilde{x}^n) \neq f(\tilde{x}^n)$, найдется набор \tilde{a} из T , для которого выполнено неравенство $f(\tilde{a}) \neq g(\tilde{a})$ (соответственно, для любых двух неравных функций g, h , порождённых источником U (также в качестве одной из этих функций может быть выбрана исходная функция f), найдется набор \tilde{a} из T , для которого выполнено неравенство $g(\tilde{a}) \neq h(\tilde{a})$). Тест минимальной длины называется *минимальным*. Обозначим через $L^{detect}(U, f(\tilde{x}^n))$ (соответственно, через $L^{diagn}(U, f(\tilde{x}^n))$) длину минимального проверяющего (соответственно, диагностического) теста относительно источника неисправностей U .

Определим *функции Шеннона длины проверяющего и диагностического теста относительно источника неисправностей U* :

$$L^{detect}(n) = \max_{f(\tilde{x}^n) \in P_2^n} L^{detect}(U, f(\tilde{x}^n)), \quad (1)$$

$$L^{diagn}(n) = \max_{f(\tilde{x}^n) \in P_2^n} L^{diagn}(U, f(\tilde{x}^n)). \quad (2)$$

¹ ООО "Микропроект".

² Факультет вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова.

* Работа выполнена при финансовой поддержке Московского центра фундаментальной и прикладной математики (проект <<Оценки сложностных характеристик булевых функций и графов>>), РФФИ (проект №18-01-00800 А) и Госбюджетной темы НИР № 5.4.19 факультета ВМК МГУ имени М.В. Ломоносова.

1. Сдвиги переменных влево с открывающимися значениями

Рассмотрим источник неисправностей U_n^{shifts} , способный действовать на булеву функцию $f(x_1, \dots, x_n)$ следующим образом. Источником выбираются (произвольным образом) число $k = 1, \dots, n$ и набор $\tilde{\gamma} = (\gamma_1, \dots, \gamma_n) \in E_2^n$ и вместо значения функции $f(\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_n)$ вычисляется значение $f(\alpha_{k+1}, \dots, \alpha_n, \gamma_{n-k+1}, \dots, \gamma_n)$ (то есть функцией неисправности будет функция $f_{k, \tilde{\gamma}}(x_1, \dots, x_n) = f(x_{k+1}, \dots, x_n, \gamma_{n-k+1}, \dots, \gamma_n)$). Определим

$$W_f = \{f_{k, \tilde{\gamma}}(\tilde{x}^n) \mid k = 1, \dots, n, \tilde{\gamma} \in E_2^n\}.$$

Назовем такой источник неисправностей U_n^{shifts} *источником сдвигов переменных влево с открывающимися значениями*.

Теорема 1. *При любом $n \in \mathbb{N}$ имеет место равенство $L^{detect}(U_n^{shifts}, n) = 2$.*

Доказательство. Рассмотрим произвольную функцию $f(\tilde{x}^n) \in P_2^n$. Заметим, что если эта функция тождественно равна константе, то никакие сдвиги переменных влево с открывающимися значениями не обнаруживаются, длина проверяющего теста в этом случае равна нулю. Будем, далее, считать, что у функции $f(\tilde{x}^n)$ есть хотя бы одна существенная переменная. Пусть x_q – существенная переменная с минимальным индексом. Тогда составим множество T из произвольной пары n -разрядных двоичных наборов $\tilde{\beta}' = (\beta_1, \dots, \beta_{q-1}, 0, \beta_{q+1}, \dots, \beta_n)$ и $\tilde{\beta}'' = (\beta_1, \dots, \beta_{q-1}, 1, \beta_{q+1}, \dots, \beta_n)$, отличающихся лишь значениями переменной x_q и таких, что $f(\tilde{\beta}') \neq f(\tilde{\beta}'')$. Докажем, что T – полный проверяющий тест относительно сдвигов переменных функции $f(x_1, x_2, \dots, x_n)$ влево (с открывающимися значениями). Поскольку при любых $k = 1, \dots, n$ и $\tilde{\gamma} = (\gamma_1, \dots, \gamma_n) \in E_2^n$ функция $f_{k, \tilde{\gamma}}(x_1, \dots, x_n) = f(x_{k+1}, \dots, x_n, \gamma_{n-k+1}, \dots, \gamma_n)$ существенно от переменной x_q не зависит (в силу выбора x_q), то $f_{k, \tilde{\gamma}}(\tilde{\beta}') = f_{k, \tilde{\gamma}}(\tilde{\beta}'')$, и, значит, оба этих значения отличаются от одного из значений $f(\tilde{\beta}')$ и $f(\tilde{\beta}'')$, откуда следует верхняя оценка $L^{shifts, detect}(n) \leq 2$. Нижняя оценка мгновенно получается из того, что полный проверяющий тест относительно сдвигов переменных функции $f_0(x_1, x_2, \dots, x_n) = x_1$ влево не может состоять из одного набора. Теорема доказана.

Теорема 2. *При $n \in \mathbb{N}$ имеют место неравенства $c' \cdot 2^{n/2} - 1 \leq L^{diagn}(U_n^{shifts}, n) \leq c \cdot 2^{n/2}$, где при n нечетном $c' = \sqrt{2}/2$ и $c = 2\sqrt{2}$, а при n четном $c' = 1$ и $c = 3$.*

Доказательство. Верхняя оценка. Положим $k' = \lfloor \frac{n}{2} \rfloor$. Легко видеть, что для любых $k = k', k' + 1, \dots, n$, набора $\tilde{\gamma} = (\gamma_1, \dots, \gamma_n) \in E_2^n$ и набора $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n) \in E_2^n$ значение $f_{k, \tilde{\gamma}}(\tilde{\alpha})$ равно значению

$f_{k,\tilde{\gamma}}(\tilde{0}^k, \alpha_{k+1}, \dots, \alpha_n)$. Поэтому все такие не равные друг другу функции неисправности $f_{k,\tilde{\gamma}}$ заведомо попарно отличаются на наборах вида $(\tilde{0}^{k'}, \beta_{k'+1}, \dots, \beta_n)$ $((\beta_{k'+1}, \dots, \beta_n) \in E_2^{n-k'})$, а число этих наборов есть $2^{n-k'} = O(\sqrt{2^n})$. Количество остальных попарно неравных функций из $W_f \cup \{f\}$ не больше $2^0 + 2^1 + \dots + 2^{k'-1} = 2^{k'} - 1$, поэтому их можно отличить друг от друга и от всех упомянутых ранее функций на не более чем $2^{k'} - 1 + \min(2^{n-k'}, 2^{k'} - 1)$ наборах, так что всего потребуется не более $2^{n-k'} + 2^{k'} - 1 + \min(2^{n-k'}, 2^{k'} - 1) \leq c \cdot 2^{n/2}$ наборов, где $c = 2\sqrt{2}$ при нечетном n и $c = 3$ при четном n . Верхняя оценка доказана.

Нижняя оценка. Рассмотрим (пользуясь идеей из [1]) функцию

$$h(\tilde{x}^n) = \bigvee_{(\sigma_1, \dots, \sigma_{k'}) \in E_2^{k'} \setminus \{\tilde{1}^{k'}\}} x_1^{\sigma_1} x_2^{\sigma_2} \dots x_{k'}^{\sigma_{k'}} x_{k'+1}^{\sigma_1} \dots x_{2k'}^{\sigma_{k'}} x_{2k'+1} \dots x_n. \quad (3)$$

Ясно, что $h(\tilde{x}^n) \not\equiv 0$ и что среди функций из W_h есть тождественный нуль. Замечая, что при $\tilde{\gamma} = (\tilde{1}^{k'}, \gamma_{k'+1}, \dots, \gamma_{2k'}, \tilde{1}^{n-2k'})$ и $\tilde{\gamma} \neq \tilde{1}^n$ функция $h_{n-k',\tilde{\gamma}}(\tilde{x}^n)$ отличается от тождественного нуля только на наборах вида $(\alpha_1, \dots, \alpha_{n-k'}, \gamma_{k'+1}, \dots, \gamma_{2k'})$, делаем вывод, что в любой диагностический тест для функции h должен войти хотя бы один набор такого вида для каждого набора $\tilde{\gamma} = (\tilde{1}^{k'}, \gamma_{k'+1}, \dots, \gamma_{2k'}, \tilde{1}^{n-2k'})$ и $\tilde{\gamma} \neq \tilde{1}^n$, откуда и вытекает нижняя оценка вида $L^{shifts,diagn}(n) \geq 2^{k'} \geq c' \cdot 2^{n/2} - 1$, где $c' = \sqrt{2}/2$ при нечетном n и $c' = 1$ при четном n . Теорема доказана.

Следствие. $L^{diagn}(U_n^{shifts}, n) = \Theta(\sqrt{2^n})$.

2. Сдвиги переменных влево на k позиций с открывающимися значениями

Теперь рассмотрим источник неисправностей $U_{n,k}^{shifts}$, способный действовать на булеву функцию $f(x_1, \dots, x_n)$ следующим образом. Источником выбирается (произвольным образом) набор $\tilde{\gamma} = (\gamma_1, \dots, \gamma_k)$, и вместо значения функции $f(\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_n)$ вычисляется значение $f(\alpha_{k+1}, \dots, \alpha_n, \gamma_1, \dots, \gamma_k)$, то есть функцией неисправности будет функция $f_{\tilde{\gamma}}(x_1, \dots, x_n) = f(\alpha_{k+1}, \dots, \alpha_n, \gamma_1, \dots, \gamma_k)$. Определим $V_{\tilde{\gamma}} = \{f_{\tilde{\gamma}}(x_1, x_2, \dots, x_n) \mid \tilde{\gamma} = (\gamma_1, \dots, \gamma_k) \in E_2^k\}$. Назовем такой источник неисправностей $U_{n,k}^{shifts}$ *источником сдвигов переменных влево на k позиций (с открывающимися значениями)*.

Теорема 3. При любом $n \in \mathbb{N}$ имеет место равенство $L^{detect}(U_{n,k}^{shifts}, n) = 2$.

Доказательство аналогично доказательству теоремы 1.

Теорема 4. При любых натуральных $n, k, 1 \leq k \leq n$, имеют место неравенства: $\min(2^k - 1, 2^{n-k}) \leq L^{diagn}(U_{n,k}^{shifts}, n) \leq \min(2^k, 2^{n-k} + 1)$.

Доказательство. Верхняя оценка. Заметим, что в таблице неисправностей с учетом исходной функции имеется не более $2^k + 1$ функций, поэтому длина теста не больше, чем 2^k . С другой стороны, первые k переменных у всех функций неисправности (кроме исходной) являются фиктивными, поэтому эти функции в случае неравенства заведомо отличаются друг от друга на 2^{n-k} наборах. Еще один набор требуется, чтобы при необходимости отличить исходную функцию от единственного класса эквивалентности (по равенству) функций, неравных ей, но неотличимых от нее на выбранных 2^{n-k} наборах.

Докажем нижнюю оценку. Рассмотрим следующую функцию:

$$h(\tilde{x}^n) = \begin{cases} \bigvee_{(\sigma_1, \dots, \sigma_k) \in E_2^k \setminus \{(1, \dots, 1)\}} \bar{x}_1 \dots \bar{x}_{n-2k} x_{n-2k+1}^{\sigma_1} \dots x_{n-k}^{\sigma_k} x_{n-k+1}^{\sigma_1} \dots x_n^{\sigma_k}, & k \leq \lfloor \frac{n}{2} \rfloor, \\ \bigvee_{(\sigma_1, \dots, \sigma_{n-k}) \in E_2^{n-k}} x_1^{\sigma_1} \dots x_{n-k}^{\sigma_{n-k}} \bar{x}_{n-k+1} \dots \bar{x}_k x_{k+1}^{\sigma_1} \dots x_n^{\sigma_{n-k}}, & k > \lfloor \frac{n}{2} \rfloor. \end{cases} \quad (4)$$

Рассмотрим случай $k \leq \lfloor \frac{n}{2} \rfloor$. Ясно, что функция $f_{k, \tilde{1}}$ из $V_{\tilde{\gamma}}$ есть тождественный ноль. Для того чтобы отличить функцию неисправности $f_{k, \tilde{\gamma}}$ от тождественного нуля ($\tilde{\gamma} = (\gamma_1, \dots, \gamma_k) \neq \tilde{1}^k$), следует включить в тест хотя бы один набор вида $(\alpha_1, \dots, \alpha_k, \tilde{0}^{n-2k}, \gamma_1, \dots, \gamma_k)$, то есть в тест должно входить не менее $2^k - 1$ наборов, а это количество меньше, чем 2^{n-k} . Отсюда вытекает нижняя оценка.

Рассмотрим случай $k > \lfloor \frac{n}{2} \rfloor$. Ясно, что функция $f_{k, \tilde{1}}$ из $V_{\tilde{\gamma}}$ есть тождественный ноль. Для того чтобы отличить функцию неисправности $f_{k, \tilde{\gamma}}$ от тождественного нуля ($\tilde{\gamma} = (\tilde{0}^{2k-n}, \gamma_{2k-n+1}, \dots, \gamma_k)$; заметим: при этом $(\tilde{0}^{2k-n}, \gamma_{2k-n+1}, \dots, \gamma_k) \neq \tilde{1}^k$), следует включить в тест хотя бы один набор вида $(\alpha_1, \dots, \alpha_{2k-n}, \gamma_{2k-n+1}, \dots, \gamma_k)$, то есть в тест должно входить не менее 2^{n-k} наборов, а это количество не больше, чем $2^k - 1$. Отсюда вытекает нижняя оценка. Теорема доказана.

3. Константные неисправности на входах схем

Для всякого набора $\tilde{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_k) \in E_2^k$ положим $v(\tilde{\varepsilon}) = \sum_{i=1}^k \varepsilon_i 2^{k-i}$. Источником U^c константных неисправностей на входах схем способен действовать на схему, реализующую булеву функцию $f(x_1, \dots, x_n)$, следующим образом. Источником выбираются (произвольно) переменные из списка x_1, \dots, x_n и вместо выбранных переменных подставляются произвольные константы. Пусть $k \in \{1, \dots, n\}$. Источником U_k^{lc} локальных константных k -кратных неисправностей на входах схем способен действовать на схему, реализующую булеву функцию

$f(x_1, \dots, x_n)$, следующим образом. Источником выбирается (произвольно) двоичный набор $\tilde{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_k) \in E_2^k$, где $k \leq n$, а также натуральное число m , $1 \leq m \leq n - k + 1$, и вместо функции $f(x_1, \dots, x_m, \dots, x_{m+k-1}, \dots, x_n)$ вычисляется $f_{v(\tilde{\varepsilon}),k,m}(x_1, \dots, x_n) = f(x_1, \dots, x_{m-1}, \varepsilon_1, \dots, \varepsilon_k, x_{m+k}, \dots, x_n)$. Определим $W_{fk} = \{f_{v(\tilde{\varepsilon}),k,m}(x_1, x_2, \dots, x_n) \mid \tilde{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_k) \in E_2^k, m = 1, \dots, n - k + 1\} \cup \{f(x_1, x_2, \dots, x_n)\}$.

Теорема 5. Для любых натуральных k, n таких, что $1 \leq k \leq n/2$, справедливо неравенство $L^{diag}(U_k^{lc}, n) \geq \frac{2^{k+1}(n-k+1)-2}{(n-k+2)}$.

Доказательство. Рассмотрим функцию

$$f(\tilde{x}) = V_{(\sigma_1, \dots, \sigma_k) \in E_2^k} x_1^{\sigma_1} \dots x_k^{\sigma_k} x_{k+1}^{\sigma_{k+1}} \dots x_n^{\sigma_n}, \quad (5)$$

в которой для любого $r, r = k + 1, \dots, n$, выполнено равенство $\sigma_r = \sigma_{r'}$, где $r' \in \{1, \dots, k\}$, и $r' \equiv r \pmod{k}$. Упорядочим функции из множества W_{fk} следующим образом: $f, f_{0,k,1}, f_{1,k,1}, \dots, f_{2^k-1,k,1}, f_{0,k,2}, f_{1,k,2}, \dots, f_{2^k-1,k,2}, \dots, f_{0,k,n-k+1}, f_{1,k,n-k+1}, \dots, f_{2^k-1,k,n-k+1}$.

Столбцы значений этих функций, взятых в указанном порядке, образуют матрицу M_0 размеров $2^n \times (2^k(n - k + 1) + 1)$. Матрица M_0 состоит из столбца значений функции f и из $s = n - k + 1$ блоков столбцов по $t = 2^k$ столбцов в каждом блоке, причем столбцы одного блока соответствуют всем функциям вида $f_{i,k,m}$, у которых третьи индексы попарно равны. Легко заметить, что в условиях теоремы для каждого двоичного набора $\tilde{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_k)$ и для каждого $m, 1 \leq m \leq n - k + 1$, функция $f_{v(\tilde{\varepsilon}),k,m}(x_1, x_2, \dots, x_n)$ имеет вид:

$$f_{v(\tilde{\varepsilon}),k,m}(x_1, x_2, \dots, x_n) = x_1^{\delta_1} \dots x_{m-1}^{\delta_{m-1}} x_{m+k}^{\delta_{m+k}} \dots x_n^{\delta_n}. \quad (6)$$

Причем для любого $r, r \in \{1, \dots, m-1\} \cup \{m+k, \dots, n\}$, выполнено равенство $\delta_r = \delta_{r'}$, где $r' \in \{1, \dots, k\}$ и $r' \equiv r - m + 1 \pmod{k}$. Поэтому (так как $k < n$) в каждой строке матрицы M_0 в пределах любого одного блока имеется не более одной единицы. Одинаковых столбцов в матрице M_0 нет. Действительно, предположение о наличии одинаковых столбцов в разных блоках противоречит тому, что соответствующие этим столбцам функции являются элементарными конъюнкциями различных множеств переменных. Предположение о наличии одинаковых столбцов в одном блоке противоречит тому, что в силу условия $k \leq n/2$ соответствующие этим столбцам функции являются элементарными конъюнкциями равных множеств переменных, но при этом наборы степеней переменных из этих конъюнкций различны. Столбец значений исходной функции очевидным образом отличен от столбца значений любой из функций вида $f_{i,k,m}$. Пусть в этой матрице M_0 выбрано l строк так, что все столбцы в составленной из этих строк таблице M' попарно различны (т. е. соответствующие этим l

строкам наборы значений входных переменных образуют диагностический тест), а l – минимально возможное. Удалим в M' первый столбец и линейно переупорядочим оставшиеся в M' столбцы (не переставляя их) по неубыванию веса, т. е. числа единиц в столбце. Тогда, поскольку все столбцы разные, среди всех столбцов в первом (в соответствии с указанным линейным порядком) – не менее нуля единиц, в следующих l – не менее чем по одной единице в каждом, в остальных $ts - (l + 1)$ – не менее чем по две единицы в каждом (иначе были бы равные столбцы). Значит, общее число единиц в таблице не менее чем $l + 2(ts - l - 1)$. С другой стороны, так как число единиц в каждой строке меньше либо равно s , то общее число единиц в матрице меньше либо равно sl . Получаем неравенство: $sl \geq l + 2 \cdot (ts - l - 1)$, т. е. $l \geq \frac{2ts-2}{s+1}$. Подставляя значения t, s , получаем: $L^{diagn}(U_k^{lc}, n) \geq L^{diagn}(U_k^{lc}, f(\tilde{x}^n)) \geq \frac{2^{k+1}(n-k+1)-2}{n-k+2}$.

Теорема доказана.

Теорема 6. При $n \rightarrow \infty, k = k(n) \rightarrow \infty, 1 \leq k \leq n/2, \log_2 n = o(k)$ справедливо асимптотическое равенство:

$$\log_2 L^{diagn}(U_k^{lc}, n) = k \cdot (1 + o(1)).$$

Доказательство. По теореме 5 имеет место неравенство $\log_2 L^{diagn}(U_k^{lc}, n) = k \cdot (1 + o(1))$. Для любой булевой функции $f(x_1, x_2, \dots, x_n)$ число попарно неравных функций в множестве W_{fk} не превосходит $(n - k + 1) \cdot 2^k + 1$, а, значит, в условиях данной теоремы для любой булевой функции $f(x_1, x_2, \dots, x_n)$ имеет место неравенство $\log_2 L^{diagn}(U_k^{lc}, f(\tilde{x}^n)) \leq \log_2((n - k + 1) \cdot 2^k) = k \cdot (1 + o(1))$, откуда и вытекает требуемое. Теорема доказана.

В статье [1] В.Н. Носковым установлены оценки $\frac{2^{n/2}}{2\sqrt{n}} \leq L^{diagn}(U^c, n) \leq 4(1+n)^3 \cdot 2^{0,773n}$. В той же статье [2, сноска на стр. 74] В.Н. Носков отмечал, что можно доказать неравенство $L^{diagn}(U^c, n) \geq 2^{\lfloor n/2 \rfloor} - 1$. В статье [2] К.А. Попков получил следующую оценку $L^{diagn}(U^c, n) \geq 2^{\frac{n}{2}}$, если n чётно, $L^{diagn}(U^c, n) \geq \left\lfloor \frac{2\sqrt{2}}{3} 2^{\frac{n}{2}} \right\rfloor$, если n нечетно. Полагая $k = \left\lfloor \frac{n}{2} \right\rfloor$, получим из теоремы 5 чуть более сильную нижнюю оценку $L^{diagn}(U^c, n) \geq L^{diagn}(U_{\lfloor n/2 \rfloor}^{lc}, n) \geq \frac{2^{\lfloor n/2 \rfloor + 1} (\lfloor n/2 \rfloor + 1) - 2}{(\lfloor n/2 \rfloor + 2)} \geq 2 \cdot 2^{\lfloor n/2 \rfloor} \cdot (1 + o(1))$ при условии стремления n к бесконечности. Значит, имеет место

Теорема 7. При $n \rightarrow \infty$ справедливо асимптотическое неравенство $L^{diagn}(U^c, n) \geq 2 \cdot 2^{\lfloor n/2 \rfloor} \cdot (1 + o(1))$.

Заключение

В настоящей статье получены оценки функций Шеннона длин тестов при специальных сдвиговых неисправностях на входах схем, а также при константных неисправностях на входах схем. В частности, установлено точное значение функции Шеннона длины проверяющего теста относительно сдвигов (всех и на k позиций) переменных влево с открывающимися значениями, что свидетельствует о легкотестируемости всех булевых функций относительно обнаружения таких неисправностей. Кроме того, установлен порядок роста $\Theta(\sqrt{2^n})$ функции Шеннона длины диагностического теста относительно сдвигов переменных влево с открывающимися значениями; далее, с точностью до аддитивной константы 1 найдено значение функции Шеннона длины диагностического теста относительно сдвигов переменных на k позиций влево с открывающимися значениями. Получена нетривиальная нижняя оценка функции Шеннона длины диагностического теста относительно k -кратных локальных константных неисправностей на входах схем, позволившая улучшить известные нижние оценки функции Шеннона длины диагностического теста относительно константных неисправностей на входах схем.

Литература

1. Носков В.Н. Диагностические тесты для входов логических устройств // Дискрет. анализ. – Вып. 26. – Новосибирск: ИМ СО АН СССР, 1974. – С. 72-83.
2. Попков К.А. Нижние оценки длин полных диагностических тестов для схем и входов схем // Прикладная дискретная математика. – 2016. – №4(34). – С. 65-73.