Д. С. Романов

О ПРОВЕРЯЮЩИХ ТЕСТАХ ДЛЯ КОНСТАНТНЫХ НЕИСПРАВНОСТЕЙ НА ВХОДАХ СХЕМЫ СЧЕТЧИКА ЧЕТНОСТИ*

В работе изучается длина минимальных проверяющих тестов относительно источников неисправностей некоторых типов, вызывающих произвольные константные неисправности на входах схемы счетчика четности порядка n.

Счетчиком четности порядка n называется линейная функция $f_n(x_1, x_2, \ldots, x_n) = x_1 \oplus x_2 \oplus \ldots \oplus x_n$. Константная неисправность на входах схемы, реализующей булеву функцию, заключается в замене некоторых переменных этой булевой функции константами. Поскольку вид схемы при этом неважен, в дальнейшем будем говорить о константных неисправностях самой булевой функции, не упоминая входов схем.

Множество T наборов значений переменных $x_1, \ldots, x_n$ называется проверяющим *тестом* [1] для неисправностей функции $f(x_1, \ldots, x_n)$ относительно источника неисправностей U тогда и только тогда, когда любая неравная функции f функция f', которая может быть получена из f в результате действия источника неисправностей U, отличается на множестве T от функции f. *Длиной* теста называется число наборов в нем. Тест минимальной длины называется *минимальным*.

Тесты для счетчиков четности строились в целом ряде работ.

В работе О. А. Долотовой [2], см. также [3; стр. 66-83], были найдены точные значения или асимптотическое поведение длины минимальных единичных проверяющих тестов относительно константных неисправностей для самых труднотестируемых функций из всех классов Поста (в частности, было доказано, что длина минимального единичного проверяющего теста относительно произвольных константных неисправностей на входах схем равна 2). В работе В. Г. Хахулина [4] доказывается, в частности, что длина минимального полного проверяющего теста относительно произвольных константных

* Работа выполнена при финансовой поддержке грантов РФФИ № 12-01-00964 и № 13-01-00958.

неисправностей на входах схем не меньше $n + 1$. В той же работе [4] приводится верхняя оценка $n+2$ длины минимального полного проверяющего теста для счетчика четности, реализованного схемой из функциональных элементов в произвольном допустимом базисе при константных неисправностях на входах функциональных элементов. (Предлагаемая в данной работе теорема 1 фактически не является новой и приводится для демонстрации более короткого доказательства нижней оценки: верхняя оценка в этой теореме тривиальна, а нижняя ранее доказывалась в [4]). В работе С. Р. Беджановой [5] доказывается существование реализующей счетчик четности порядка n схемы из функциональных элементов в стандартном базисе, допускающей проверяющий тест длины $]\log_2(n-1)[+2$ для инверсных неисправностей на выходах элементов. Упомянем также, что тесты для функции f_n, реализованной контактными схемами, изучались в работах [1; стр. 322-325], [6-10]. В статье [11] изучались тесты для линейных локальных неисправностей на входах схем. Близкие задачи возникают в теории расшифровки булевых функций и объемлющей последнюю теории изучения булевых функций по запросам (learning Boolean functions). Сложность расшифровки счетчиков четности от n переменных с помощью деревьев решений изучалась в работе [12]. Отметим, что к рассматриваемой в статье тематике примыкает и область вероятностного тестирования свойств булевых функций (testing properties of Boolean functions), в рамках которой оценивается минимальная длина вероятностного теста, позволяющего либо точно установить, что предлагаемая для тестирования функция лежит в предписанном классе («обладает заданным свойством») или находится «близко» к одной из функций предписанного класса, либо же с достаточной вероятностью установить, что предлагаемая для тестирования функция находится «далеко» от любой из функций предписанного класса (см., например, работы [13, 14]). Тестированию линейности уделено внимание в работах [14-19].

В качестве источников неисправностей в данной работе рассматриваются следующие источники:

U_r — источник неисправностей, допускающий замену не более r переменных булевой функции произвольными (булевыми) константами;

$U^{\text{п}} = U_n$ — источник неисправностей, допускающий всевозможные константные неисправности функции (тесты относительно $U^{\text{п}}$ называются *полными*);

$U^{\text{ч}}$ — источник неисправностей, допускающий замену четного числа переменных булевой функции произвольными константами;

$U^{н}$ — источник неисправностей, допускающий замену нечетного числа переменных булевой функции произвольными константами;

$U^{л}$ — источник неисправностей, допускающий *локальные* константные неисправности булевой функции, т. е. такие неисправности, при которых из того, что вместо переменных x_i и x_j $(i < j)$ подставлены константы, следует, что вместо всех переменных x_k, где $i < k < j$, подставлены константы (тесты относительно $U^{л}$ назовем *локальными*).

Длину минимального проверяющего теста для константных неисправностей функции f_n относительно источников U_r, $U^{п}$, $U^{ч}$, $U^{н}$, $U^{л}$ будем обозначать через $l_r(n)$, $l^{п}(n)$, $l^{ч}(n)$, $l^{н}(n)$, $l^{л}(n)$ соответственно.

В дальнейшем для краткости вместо слов “проверяющий тест для константных неисправностей функции f_n относительно источника неисправностей U” будем писать “тест для f_n относительно U”.

Запишем (упорядоченные некоторым образом) наборы теста T в виде матрицы $M(T)$ так, что каждый набор теста представляет собой строку матрицы $M(T)$ (при этом каждый столбец матрицы $M(T)$ будет соответствовать своей входной переменной, а подмножество множества столбцов — подмножеству множества входных переменных).

Лемма 1. *Множество T двоичных n-разрядных наборов является проверяющим тестом для константных неисправностей функции f_n относительно источника неисправностей U тогда и только тогда, когда покоординатная сумма по модулю 2 столбцов матрицы $M(T)$, соответствующих любому подмножеству множества переменных $\{x_1,\ldots,x_n\}$, которое может быть повреждено источником U, отлична от столбца из всех нулей и от столбца из всех единиц.*

Доказательство. Пусть покоординатная сумма по модулю 2 столбцов матрицы $M(T)$, соответствующих множеству переменных $\{x_{j_1}, x_{j_2},\ldots, x_{j_q}\}$ (которое источник U может в точности забить константами и которое лежит в множестве $\{x_1, \ldots, x_n\}$), равна столбцу, все элементы которого равны σ ($\sigma \in \{0,1\}$). Тогда функция $f_n(x_1,\ldots,x_n)$ на наборах из T не будет отличаться от функции, полученной из $f_n(x_1,\ldots,x_n)$ подстановкой константы σ вместо переменной x_{j_1} и константы 0 вместо переменных $x_{j_2},\ldots,x_{j_q}$. Значит, T не является проверяющим тестом.

Пусть теперь T не является проверяющим тестом для $f_n(x_1,\ldots,x_n)$ относительно источника неисправностей U. Тогда найдется функция $f'_n(x_1,\ldots,x_n)$, полученная из $f_n(x_1,\ldots,x_n)$ подстановкой (под действием U)

вместо переменных $x_{j_1}, x_{j_2}, \ldots, x_{j_q}$ булевых констант $\sigma_1, \sigma_2, \ldots, \sigma_q$ соответственно и неотличимая от $f_n(x_1, \ldots, x_n)$ на множестве T. Но так как $f_n(x_1, \ldots, x_n)$ — счетчик четности, то последнее означает, что сумма по модулю 2 тех столбцов матрицы $M(T)$, которые соответствуют столбцам переменных $x_{j_1}, x_{j_2}, \ldots, x_{j_q}$, равна столбцу, каждый элемент которого равен константе $\sigma_1 \oplus \sigma_2 \oplus \cdots \oplus \sigma_q$. Лемма доказана.

Далее для простоты обозначений вместо "$\underbrace{a_1, a_2, \ldots, a_t, a_1, a_2, \ldots, a_t, \ldots, a_1, a_2, \ldots, a_t}_{tk \text{ символов}}$" будем писать "$[a_1 a_2 \ldots a_t]^k$".

Теорема 1. *При* $n \geq 2$ $l^{\text{п}}(n) = n + 1$.

Доказательство. Верхняя оценка тривиальна (достаточно рассмотреть все наборы единичного шара с центром в наборе $([0]^n)$).

Нижняя оценка. Разобьем двоичные l-разрядные наборы на типы, отнеся к одному типу противоположные наборы. Число типов при этом будет равно 2^{l-1}. Предположим, что существует тест T длины l, $l \leq n$. Тогда число непустых подмножеств столбцов матрицы T равно $2^n - 1$, что больше, чем 2^{l-1}. Значит, суммы по модулю 2 каких-то двух различных подмножеств A и B столбцов матрицы T относятся к одному типу, а, следовательно, сумма столбцов из множества $C = (A \cup B) \setminus (A \cap B) = A \Delta B$ есть постоянный столбец, т. е. T не является тестом по лемме 1. Полученное противоречие доказывает теорему.

Изучим теперь локальные проверяющие тесты для константных неисправностей f_n. Пусть T — множество, состоящее из l двоичных n-разрядных наборов. Построим по T последовательность $R(T)$, состоящую из n разбиений множества наборов T на два блока, по следующему принципу: для всякого i, $i = \overline{1,n}$, к первому блоку i-го разбиения отнесем те наборы из T, у которых сумма по модулю 2 значений первых i переменных равна 0, а ко второму блоку — те наборы из T, у которых сумма по модулю 2 значений первых i переменных равна 1. Легко устанавливается следующий критерий.

Лемма 2. *Множество T является локальным проверяющим тестом для константных неисправностей f_n тогда и только тогда, когда в последовательности $R(T)$ все блоки непусты и попарно различны.*

Доказательство. Пустота s-го блока ($s \in \{1,2\}$) i-го разбиения в $R(T)$ равносильна тому, что на множестве T не обнаруживается ошибка, заключающаяся в забивании всех первых i переменных константами, сумма которых сравнима с s по модулю 2. Далее, равенство s_1-го блока

i-го разбиения и s_2-го блока j-го разбиения в $R(T)$ ($s_1, s_2 \in \{1,2\}$, $i < j$) равносильно тому, что на множестве T не обнаруживается ошибка, заключающаяся в забивании всех первых переменных с i-й по j-ю константами, сумма которых сравнима с $s_1 + s_2$ по модулю 2. Фактически, эта лемма является применением леммы 1 для $U = U^{\text{л}}$.

Теорема 2. *При всех натуральных n имеет место равенство*

$$l^{\text{л}}(n) =]\log_2(n+1)[+1.$$

Доказательство. Нижняя оценка. Пусть T — локальный проверяющий тест для f_n, состоящий из l двоичных n-разрядных наборов. По лемме 2 значение n не может превосходить максимальной длины последовательности разбиений l элементов на 2 блока, в которой все блоки непусты и попарно различны. Эта длина, в свою очередь, не может быть больше числа различных блоков, которые в разбиениях могут являться минимальными по мощности, т. е. $n \le \sum_{i=1}^{[l/2]} C_l^i \le 2^{l-1} - 1$, откуда $l \ge \log_2(n+1) + 1$, $l \ge]\log_2(n+1)[+1$.

Верхняя оценка. Рассмотрим сначала случай $n = 2^m$, m – целое неотрицательное. В тест T включаются два набора: $(0[0]^{2^m-1})$ и $(1[0]^{2^m-1})$ — они обеспечивают непустоту всех блоков рассматриваемой последовательности разбиений $R(T)$ и отличимость всех первых блоков разбиений от всех вторых. Остальные m наборов T (при $m \in \mathbb{N}$) строятся методом дихотомии: $([1[0]^{2^{m-1}-1}]^2)$, $([1[0]^{2^{m-2}-1}]^4)$,..., $([1[0]^{2^{m-i}-1}]^{2^i})$,..., $([10]^{2^{m-1}})$, $([1]^{2^m})$. Все $m+2$ наборов, очевидно, образуют локальный тест по лемме 2, так что в этом случае $l \le]\log_2(n+1)[+1$.

Рассмотрим теперь случай $n = 2^m - 1$, m – натуральное, $m \ge 2$. В тест T включается набор $(1[0]^{2^m-2})$ — он обеспечивает непустоту всех вторых блоков рассматриваемой последовательности разбиений $R(T)$ и отличимость всех первых блоков разбиений от всех вторых. Остальные m наборов T строятся методом дихотомии, причем все, кроме последнего, получаются из наборов с 3-го по $(m+1)$-й из пункта *а)* для того же m выбрасыванием второго разряда, а последний набор получается из $(m+2)$-го набора из пункта *а)* для того же m выбрасыванием второго разряда и инвертированием первого разряда: $(1[0]^{2^{m-1}-2}1[0]^{2^{m-1}-1})$, $(1[0]^{2^{m-2}-2}[1[0]^{2^{m-2}-1}]^3)$,..., $(1[0]^{2^{m-i}-2}[1[0]^{2^{m-i}-1}]^{2^i-1})$, ..., $(1[10]^{2^{m-1}-1})$, $(0[1]^{2^m-2})$. Легко видеть, что все первые блоки разбиений $R(T)$ также непусты и что

все блоки в $R(T)$ попарно различны. Значит, все $m+1$ наборов образуют локальный тест по лемме 2, так что и в этом случае $l \le]\log_2(n+1)[+1$.

Тест для произвольного n, $2^{m-1} < n \le 2^m - 2$, $m \ge 3$, строится по тесту T из предыдущего абзаца для того же m отбрасыванием нужного количества последних разрядов. Теорема доказана.

Теорема 3. *При натуральных n, $n \ge 2$, имеют место равенства:*

$$l^{\text{ч}}(n) = n,\ l^{\text{н}}(n) = 2.$$

Доказательство. Верхнюю оценку первого равенства по лемме 1 обеспечивает тест, состоящий из строк квадратной матрицы порядка n:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & 0 & 0 & \dots & 1 & 0 \\ 1 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Нижняя оценка доказывается аналогично нижней оценке теоремы 1 с учетом того, что число имеющих четную мощность непустых подмножеств столбцов матрицы $M(T)$ теста T равно $2^{n-1}-1$, и того, что если мощности множеств A и B четны, то мощность множества $C = A\Delta B$ также четна. Верхняя оценка второго равенства следует из рассмотрения теста $T = \{([0]^n),([1]^n)\}$, нижняя очевидна.

Следствие 1. *Для любых натуральных r и n, $n \ge 2r+1$, верны неравенства: $l_{2r-1}(n) \le l_{2r}(n) \le l_{2r+1}(n) \le l_{2r}(n) + 2$.*

Теорема 4. *При $n \ge 2$, $2 \le r \le n$ (r и n – натуральные) верны неравенства:*

$$\log_2\left(\sum_{i=1}^{[r/2]} C_n^i\right) + 1 \le l_r(n) \le \log_2\left(\sum_{i=0}^{2\cdot[r/2]-1} C_{n+1}^i\right) + 4.$$

Доказательство Нижняя оценка. Пусть T — тест длины l относительно U_r. Число непустых имеющих мощность не более $[r/2]$ подмножеств множеств столбцов матрицы теста $M(T)$ равно $\sum_{i=1}^{[r/2]} C_n^i$. Если это число больше 2^{l-1}, то найдутся два подмножества A и B, суммы (по модулю 2) столбцов которых либо равны, либо противоположны, следовательно, сумма столбцов подмножества $C = A\Delta B$ ($|C| \le r$) есть

постоянный столбец, и T — не тест по лемме 1. Значит, $\sum_{i=1}^{[r/2]} C_n^i \le 2^{l_r(n)-1}$.

Верхняя оценка. Случай четного натурального r. Отыщем при фиксированном l достаточно большое значение n, при котором существует тест T длины l для f_n относительно источника U_r. Всякое (в том числе пустое) подмножество столбцов матрицы теста, имеющее мощность не более $r-1$, запрещает попадание в матрицу теста двух столбцов, а именно, столбцов, которые в сумме по модулю 2 со столбцами указанного подмножества дают постоянный столбец. Таким образом, все $\sum_{i=0}^{r-1} C_n^i$ подмножеств запрещают попадать в матрицу теста не более чем $2\sum_{i=0}^{r-1} C_n^i$ столбцам. Если $2\sum_{i=0}^{r-1} C_n^i < 2^l$, найдется столбец, который можно добавить справа к матрице T, чтобы получить тест для f_{n+1}. Пусть n_l — максимальное из таких n, для которых выполняется последнее неравенство. Для n_l выполняются неравенства

$$2\sum_{i=0}^{r-1} C_{n_l}^i < 2^l \le 2\sum_{i=0}^{r-1} C_{n_l+1}^i .$$

Очевидно, что $n_{l-1} \le n_l$, если первое из чисел существует и $l \ge 2$. Пусть теперь $n \in [n_{l-1}; n_l]$. Тогда для такого n заведомо существует тест длины l, и при этом выполнены неравенства

$$2^{l-1} \le 2\sum_{i=0}^{r-1} C_{n_{l-1}+1}^i \le 2\sum_{i=0}^{r-1} C_{n+1}^i ,$$

откуда вытекает неравенство

$$l_r(n) \le \log_2\left(\sum_{i=0}^{2\cdot[r/2]-1} C_{n+1}^i\right) + 2.$$

Случай нечетного r выводится из следствия 1.

Следствие 2. *При $n \to \infty$ имеют место равенства:*

$$l_2(n) = \log_2 n \cdot (1+o(1)), \quad l_3(n) = \log_2 n \cdot (1+o(1)).$$

Следствие 3. *Если $n \to \infty$, $c < 1$, $r \le cn$ ($r \ge 2$; r и n – натуральные), то $l_r(n) = \Theta(\log_2 n)$. Если же $n \to \infty$, $\gamma = o(n)$, $n - \gamma(n) \le r \le n$ ($r \ge 2$; r и n – натуральные), то $l_r(n) = n \cdot (1+o(1))$.*

Следствия 2 и 3 легко вывести из результатов статьи [19; стр. 270-272, п. 3.1] и формулы Стирлинга.

Автор выражает благодарность профессору С. А. Ложкину за внимание к работе.

Литература

1. Чегис И. А., Яблонский С. В. Логические способы контроля работы электрических схем // Труды МИАН СССР. Т. LI. М., 1958. С. 270-360.

2. Долотова О. А. О сложности проверяющих тестов для классов Поста // Труды семинара по дискретной математике и ее приложениям. М.: МГУ, 1989. С. 233-244.

3. Кудрявцев В. Б., Гасанов Э. Э., Долотова О. А., Погосян Г. Р. Теория тестирования логических устройств. М.: ФИЗМАТЛИТ, 2006. 160 с.

4. Хахулин В. Г. О проверяющих тестах для счетчика четности // Дискретная математика. Т. 7, 1995. № 4. С. 51-59.

5. Беджанова С. Р. Легкотестируемые схемы для линейных функций // Вестн. Моск. ун-та. Серия 1. Матем. Механ. Т. 66, 2011. № 4. С. 57-59.

6. Мадатян Х. А. Полный тест для бесповторных контактных схем // Проблемы кибернетики. Вып. 23. М.: Наука, 1970. С. 103-118.

7. Тоноян Р. Н. О единичных тестах для контактных схем, реализующих линейные функции // Изв. АН Арм. ССР. Т. VI, № 1. 1971. С. 61-66.

8. Редькин Н. П. О полных проверяющих тестах для контактных схем // Методы дискретного анализа в исследовании экстремальных структур. Вып. 39. Новосибирск: ИМ СО АН СССР, 1983. С. 80-87.

9. Вартанян С. М. Единичные диагностические тесты для последовательных блочных схем : Дисс. … канд. физ.-мат. наук. М.: МГУ имени М. В. Ломоносова, 1987. 114 с.

10. Романов Д. С. Построение тестов и оценка их параметров для некоторых классов контактных схем : Дисс. … канд. физ.-мат. наук. М.: МГУ имени М. В. Ломоносова, 2000. 114 с.

11. Морозов Е. В., Романов Д. С. О тестах относительно локальных линейных слипаний переменных в булевых функциях // Вестник Нижегородского университета им. Н.И. Лобачевского. 2012. № 5(2). С. 151-156.

12. Ryuhei Uehara, Kensei Tsuchida, Ingo Wegener. Optimal attribute-efficient learning of disjunction, parity, and threshold functions // Computational Learning Theory (Third European Conference, EuroCOLT '97 Jerusalem, Israel, March 17–19, 1997, Proceedings). Lecture Notes in Computer Science, Volume 1208, Publisher: Springer Berlin Heidelberg, 1997, pp 171-184.

13. Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing // SIAM J. Comput., 25(2), 1996, pp 252–271.

14. Eric Blais. Testing Properties of Boolean Functions. Report (PhD thesis) CMU-CS-12-101. School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213. January 2012. 149 p.

15. Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems // J. Comput. Syst. Sci., 47, 1993, pp 549–595.

16. Mihir Bellare, Shafi Goldwasser, Carsten Lund, and Alexander Russell. Efficient probabilistically checkable proofs and applications to approximations // Proc. of the 25th Symposium on Theory of Computing, 1993, pp 294–304.

17. Mihir Bellare and Madhu Sudan. Improved non-approximability results // Proc. of the 26th Symposium on Theory of Computing, 1994, pp 184–193.

18. Mihir Bellare, Don Coppersmith, Johan Håstad, Marcos Kiwi, and Madhu Sudan. Linearity testing in characteristic two // IEEE Trans. on Information Theory, 42(6), 1996, pp 1781–1795.

19. Tali Kaufman, Simon Litsyn, and Ning Xie. Breaking the ε-soundness bound of the linearity test over GF(2) // SIAM J. on Computing, 39, 2010, pp 1988–2003.

20. Бендер Э. А. Асимптотические методы в теории перечислений // Перечислительные задачи комбинаторного анализа. М.: Мир, 1979. С. 266-311.