МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

УДК 519.718.7

О СХЕМАХ, ДОПУСКАЮЩИХ КОРОТКИЕ ЕДИНИЧНЫЕ ПРОВЕРЯЮЩИЕ ТЕСТЫ ПРИ ПРОИЗВОЛЬНЫХ НЕИСПРАВНОСТЯХ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ[1]

К. А. Попков

Институт прикладной математики им. М. В. Келдыша РАН, г. Москва, Россия

Доказано, что любую неконстантную булеву функцию от n переменных можно реализовать неизбыточной схемой из функциональных элементов в базисе $\{\&, \oplus, \neg\}$, содержащей не более одной фиктивной входной переменной и допускающей единичный проверяющий тест длины не более $2n+3$ относительно произвольных неисправностей элементов.

Ключевые слова: *схема из функциональных элементов, булева функция, неисправность, единичный проверяющий тест.*

DOI 10.17223/20710410/51/4

ON LOGIC NETWORKS ALLOWING SHORT SINGLE FAULT DETECTION TESTS UNDER ARBITRARY FAULTS OF GATES

K. A. Popkov

Keldysh Institute of Applied Mathematics, Moscow, Russia

E-mail: kirill-formulist@mail.ru

It is proved that one can implement any non-constant Boolean function in n variables by an irredundant logic network in the basis $\{\&, \oplus, \neg\}$, containing not more than one dummy input variable and allowing a single fault detection test with length not more than $2n+3$ regarding arbitrary faults of logic gates.

Keywords: *logic network, Boolean function, fault, single fault detection test.*

Введение

В работе рассматривается задача синтеза легкотестируемых схем, реализующих заданные булевы функции. Логический подход к тестированию электрических схем предложен С. В. Яблонским и И. А. Чегис в [1]; этот подход также применим к тестированию схем из функциональных элементов (СФЭ) [2–4]. Пусть имеется СФЭ S с одним выходом, реализующая булеву функцию $f(\tilde{x}^n)$, где $\tilde{x}^n = (x_1, \ldots, x_n)$. Представим, что под воздействием некоторого источника неисправностей один из элементов

[1]Работа выполнена при поддержке гранта РНФ, проект № 19-71-30004.

схемы S может перейти в неисправное состояние. В результате данная схема вместо исходной функции $f(\tilde{x}^n)$ будет реализовывать некоторую булеву функцию $g(\tilde{x}^n)$, вообще говоря, отличную от f. Все такие функции $g(\tilde{x}^n)$ называются *функциями неисправности* схемы S. *Единичным проверяющим тестом* (ЕПТ) для схемы S называется такое множество T наборов значений переменных $x_1, \ldots, x_n$, что для любой отличной от $f(\tilde{x}^n)$ функции неисправности $g(\tilde{x}^n)$ данной схемы в T найдётся набор $\tilde{\sigma}$, на котором $f(\tilde{\sigma}) \neq g(\tilde{\sigma})$. Число наборов в T называется *длиной* теста. В качестве тривиального ЕПТ длины 2^n для схемы S всегда можно взять множество, состоящее из всех двоичных наборов длины n. Единичные проверяющие тесты обычно рассматривают для *неизбыточных схем* [4, с. 110–111], т. е. для таких схем, в которых любая допустимая неисправность любого одного элемента приводит к функции неисправности, отличной от исходной функции, реализуемой данной схемой.

Любое множество булевых функций будем называть *базисом*.

Пусть зафиксированы вид неисправностей элементов и функционально полный базис B, в котором строятся схемы, и T — ЕПТ для некоторой СФЭ S в базисе B. Введём следующие обозначения [4]: $D(T)$ — длина теста T; $D(S) = \min D(T)$, где минимум берётся по всем ЕПТ T для схемы S; $D(f) = \min D(S)$, где минимум берётся по всем неизбыточным схемам S в базисе B, реализующим функцию f; $D(n) = \max D(f)$, где максимум берётся по всем булевым функциям f от n переменных, для которых определено значение $D(f)$. Функция $D(n)$ называется *функцией Шеннона* длины ЕПТ.

Ранее в качестве неисправностей функциональных элементов традиционно рассматривались константные либо инверсные неисправности на входах и/или выходах элементов. Константная неисправность на входе (выходе) функционального элемента означает, что значение на этом входе (выходе) становится равно некоторой булевой константе. Неисправности на входах и/или выходах элементов называются однотипными константными типа p, если эта константа одна и та же для каждого неисправного входа/выхода элемента и равна p, и произвольными константными, если эта константа может быть равна как 0, так и 1 для каждого неисправного входа/выхода элемента независимо от неисправностей других входов/выходов элементов. Инверсная неисправность на входе (выходе) функционального элемента означает, что значение на этом входе (выходе) меняется на противоположное по сравнению со случаем, когда данный элемент исправен.

Перечислим основные результаты, касающиеся ЕПТ для схем из функциональных элементов. Для удобства разобьём эти результаты на группы в соответствии с видом неисправностей элементов, рассматривавшихся в схемах. Предполагаем, что n — произвольное натуральное число.

1. *Однотипные константные неисправности типа p, $p \in \{0, 1\}$, на выходах элементов.* Ю. В. Бородина в [5] при $B = \{\&, \oplus, 1, 0\}$, $p = 1$ установила равенство $D(n) = 1$. В [6, теорема 2] для любого полного базиса B, содержащего монотонные булевы функции, кроме константы 1, из которых отождествлением и переименованием переменных можно получить функции $x \& y$ и $x \vee y$, а также содержащего функции вида $\overline{x}_1 \vee h$, где h — произвольная булева функция, и для любого $n \geqslant 2$ получено равенство $D(n) = 2$ при $p = 1$. В [7] при $B = \{\&, \neg\}$ и любых $p \in \{0, 1\}$, $n \geqslant 2$ доказано равенство $D(n) = 3$.

2. *Произвольные константные неисправности на выходах элементов.* В [4, с. 116, теорема 10] с использованием метода синтеза СФЭ, предложенного С. М. Редди [8], для базиса $B = \{\&, \oplus, 1, 0\}$ получена оценка $D(n) \leqslant n + 3$. В дальнейшем этот результат

был обобщён С. С. Колядой в [9, 10] на случай произвольного полного конечного базиса B при $n \geqslant 3$. Д. С. Романов в [11] для любого полного базиса B установил соотношение $2 \leqslant \hat{D}(n) \leqslant 4$; наличие крышки над буквой D обусловлено тем, что в указанной работе рассматривается несколько другое определение неизбыточных схем. В [12, теорема 1] заявлено получение неравенства $\hat{D}(n) \leqslant 3$ для схем в произвольном полном конечном базисе при $n \geqslant 2$. В [6, теорема 4] для произвольного полного базиса B, состоящего из функций от не более чем двух переменных, доказано неравенство $D(n) \geqslant 3$ при $n \geqslant 3$. В [13, следствие 1] при $B = \{x\&y, \overline{x}, x \oplus y \oplus z\}$ установлено, что $D(n) = 2$.

3. *Инверсные неисправности на выходах элементов.* С. В. Коваценко для базиса $B = \{\&, \oplus, 1, 0\}$ установил равенство $D(n) = 1$ [14]. Н. П. Редькин в [15] при $B = \{\&, \vee, \neg\}$ получил оценку $D(n) \leqslant 2$, а в [16] для схем в произвольном полном конечном базисе — оценку $D(n) \leqslant 3$.

4. *Однотипные константные неисправности типа* 0 *на входах и выходах элементов.* В [17, следствие 1] для базиса $B = \{xyz \vee \overline{x}\,\overline{y}\,\overline{z}, \overline{x}\}$ установлено равенство $D(n) = 2$ (в предположении, что параметр k, определённый в указанной работе и равный максимально возможному числу неисправностей в схемах, равен 1. Точно так же этот параметр определяется в работе [20], ссылку на которую см. в следующем абзаце).

5. *Произвольные константные неисправности на входах и выходах элементов.* В рассуждениях на с. 116 работы [4], следующих после формулировки теоремы 10, показано, что $D(n) \leqslant n + 3$ для схем в базисе $\{\&, \oplus, 1, 0\}$. В [18, 19] для схем в любом из базисов $\{\&, \oplus, 1\}$, $\{\&, \oplus, \sim\}$ получено неравенство $D(n) \leqslant 16$. В [20, следствие 2] (при $k = 1$) для базиса $B = \{\varphi(x, y, z, t), x \sim y, \overline{x}, 0\}$, где $\varphi(x, y, z, t)$ — некоторая булева функция, и любого $n \geqslant 2$ установлено равенство $D(n) = 3$.

6. *Инверсные неисправности на входах и выходах элементов.* В [21, утверждение 2] доказано равенство $D(n) = 1$ при $B = \{\&, \oplus, 1\}$.

В отличие от всех перечисленных работ, в данной работе рассматриваются произвольные неисправности функциональных элементов: предполагается, что каждый неисправный элемент E вместо исходной приписанной ему булевой функции $\varphi_E(\tilde{x}^m)$ реализует произвольную другую булеву функцию $\varphi'_E(\tilde{x}^m)$ (от своих входов). Таким образом, элемент E может находиться в любом (неизменном в ходе тестирования) из $2^{2^m} - 1$ неисправных состояний, характеризующихся функцией $\varphi'_E(\tilde{x}^m)$. Например, в случае константной неисправности типа p (в случае инверсной неисправности) на выходе этого элемента имеем $\varphi'_E \equiv p$ (соответственно $\varphi'_E = \overline{\varphi}_E$), а в случае константной неисправности типа p (инверсной неисправности) на входе элемента E, отвечающем переменной x_1, имеем $\varphi'_E(\tilde{x}^m) = \varphi_E(p, x_2, \ldots, x_m)$ (соответственно $\varphi'_E(\tilde{x}^m) = \varphi_E(\overline{x}_1, x_2, \ldots, x_m)$).

В соответствии с [22, с. 105] будем говорить, что СФЭ *содержит k фиктивных входных переменных и реализует функцию $f(\tilde{x}^n)$*, если данная схема содержит k входных переменных, отличных от переменных $x_1, \ldots, x_n$, и реализует булеву функцию, не зависящую существенно от этих k переменных и равную функции $f(\tilde{x}^n)$. Будем также предполагать, что все наборы из любого ЕПТ для такой схемы имеют длину $n+k$ (по общему числу её входных переменных).

Введём обозначения $\tilde{0}^l = \underbrace{0, \ldots, 0}_{l}$, $\tilde{1}^l = \underbrace{1, \ldots, 1}_{l}$, где $l \in \mathbb{N} \cup \{0\}$. В случае $l = 0$ они обозначают пустую строку: например, $(\tilde{1}^n, \tilde{0}^0) = (\tilde{1}^n)$.

Будем говорить, что функциональный элемент E является *верхним* (*нижним*) элементом некоторой цепочки, если ни один вход элемента E не соединён с выходом какого-то элемента из этой цепочки (соответственно если выход элемента E не соединён ни с одним входом ни одного элемента из этой цепочки).

Вместо «вход схемы S, отвечающий переменной x_i» для краткости будем писать «вход „ x_i“ схемы S».

Формулировка и доказательство основного результата

Рассмотрим базис $B = \{\&, \oplus, \neg\}$. Любой функциональный элемент, реализующий функцию вида $x\&y$ (вида $x \oplus y$, $\overline{x}$) от своих входов, будем называть *конъюнктором* (соответственно *сумматором*, *инвертором*). Вход любого конъюнктора или сумматора, отвечающий переменной x, будем считать *левым*, а другой вход этого элемента — *правым*. Отметим, что для любой булевой переменной x справедливо тождество

$$\overline{x} \equiv x \oplus 1. \tag{1}$$

Сформулируем основной результат данной работы.

Теорема 1. Любую неконстантную булеву функцию $f(\tilde{x}^n)$ можно реализовать:

1) неизбыточной СФЭ в базисе B, содержащей одну фиктивную входную переменную и допускающей ЕПТ длины не более $2n + 4$, подмножеством которого является множество $\{(\tilde{0}^r, \tilde{1}^{n+1-r}), (\tilde{1}^s, 0, \tilde{1}^{n-s}) : r \in \{0, \dots, n+1\}, s \in \{1, \dots, n\}\}$;
2) неизбыточной СФЭ в базисе B, содержащей одну фиктивную входную переменную и допускающей ЕПТ длины не более $2n + 3$.

Замечание 1. Константные булевы функции ни для какого $k \in \mathbb{N} \cup \{0\}$ нельзя реализовать неизбыточными СФЭ в базисе B, содержащими не более k фиктивных входных переменных. Действительно, константная неисправность типа α на выходе выходного элемента любой схемы в базисе B, содержащей k' фиктивных входных переменных и реализующей функцию $f(\tilde{x}^n) \equiv \alpha$, где $0 \leqslant k' \leqslant k$, $\alpha \in \{0, 1\}$, т. е. схемы, реализующей функцию $f'(\tilde{x}^{n+k'}) \equiv \alpha$, приводит к тривиальной функции неисправности $g(\tilde{x}^{n+k'}) \equiv \alpha$.

Замечание 2. У автора есть гипотеза, что любую неконстантную булеву функцию $f(\tilde{x}^n)$ можно реализовать неизбыточной СФЭ (без фиктивных входных переменных) в базисе B, допускающей ЕПТ линейной по n длины. Утверждение 1 теоремы 1 сформулировано именно с целью его использования в предполагаемом доказательстве данной гипотезы.

Для доказательства теоремы 1 введём некоторые обозначения и докажем две вспомогательные леммы. Пусть $f(\tilde{x}^n)$ — произвольная неконстантная булева функция. Представим её полиномом Жегалкина

$$f(\tilde{x}^n) = K_1 \oplus \ldots \oplus K_m \oplus c, \tag{2}$$

где $m \geqslant 1$; $c \in \{0, 1\}$; K_1 — самая короткая конъюнкция в этом полиноме. Пусть $K_i = x_{j_1(i)}\& \ldots \&x_{j_{t_i}(i)}$, где $i = 1, \dots, m$ и

$$1 \leqslant j_1(i) < \ldots < j_{t_i}(i) \leqslant n; \tag{3}$$

$\tilde{\sigma}_{K_1}$ — двоичный $(n+1)$-разрядный набор, содержащий единицы только в компонентах с номерами $j_1(1), \dots, j_{t_1}(1)$, а $f^{(+1)}(\tilde{x}^{n+1})$ — булева функция, не зависящая существенно от переменной x_{n+1} и равная функции $f(\tilde{x}^n)$.

В случае $m \geqslant 2$ введём следующие обозначения: $h(\tilde{x}^n) = K_2 \oplus \ldots \oplus K_m$;

$$a = \begin{cases} 1, & \text{если } K_1 \leqslant h \text{ или } K_1 \leqslant h \oplus 1, \\ 0 & \text{иначе.} \end{cases}$$

Неравенство $f_1 \leqslant f_2$, где $f_1(\tilde{x}^n)$, $f_2(\tilde{x}^n)$ — булевы функции, означает, что $f_1(\tilde{\pi}) \leqslant f_2(\tilde{\pi})$ для любого двоичного n-разрядного набора $\tilde{\pi}$.

Лемма 1. Существует такой двоичный n-разрядный набор $\tilde{\rho}$, что в случае $a = 1$ выполнены равенства $K_1(\tilde{\rho}) = 0$ и $h(\tilde{\rho}) = 1$, а в случае $a = 0$ — равенства $K_1(\tilde{\rho}) = 1$ и $h(\tilde{\rho}) = \overline{h(\tilde{1}^n)}$.

Доказательство. Пусть сначала $a = 1$. Заметим, что функция K_1 отлична от функции h, поскольку в противном случае в силу (2) выполнялось бы соотношение

$$0 \equiv K_1 \oplus h = K_1 \oplus K_2 \oplus \ldots \oplus K_m = f \oplus c,$$

однако это противоречит тому, что функция f отлична от константы c. Кроме того, функция h отлична от константы 0 в силу единственности представления каждой булевой функции полиномом Жегалкина [23, с. 32]. Равенство $a = 1$ влечёт за собой выполнение одного из двух неравенств: $K_1 \leqslant h$ или $K_1 \leqslant h \oplus 1$. В случае $K_1 \leqslant h$ с учётом различия функций K_1 и h существует такой n-разрядный набор $\tilde{\rho}$, для которого $K_1(\tilde{\rho}) = 0$ и $h(\tilde{\rho}) = 1$, что и требовалось доказать. В случае $K_1 \leqslant h \oplus 1$ возьмём в качестве $\tilde{\rho}$ любой набор, на котором функция $h(\tilde{x}^n)$ принимает значение 1. Тогда

$$K_1(\tilde{\rho}) \leqslant h(\tilde{\rho}) \oplus 1 = 1 \oplus 1 = 0,$$

т. е. $K_1(\tilde{\rho}) = 0$ и $h(\tilde{\rho}) = 1$, что и требовалось доказать.

Пусть теперь $a = 0$. Тогда не выполнено ни одно из неравенств $K_1 \leqslant h$, $K_1 \leqslant h \oplus 1$, поэтому существуют такие n-разрядные наборы $\tilde{\pi}_1$ и $\tilde{\pi}_2$, что $K_1(\tilde{\pi}_1) = K_1(\tilde{\pi}_2) = 1$, $h(\tilde{\pi}_1) = 0$ и $h(\tilde{\pi}_2) \oplus 1 = 0$, т. е. $h(\tilde{\pi}_2) = 1$. Положим

$$\tilde{\rho} = \begin{cases} \tilde{\pi}_1, & \text{если } h(\tilde{1}^n) = 1, \\ \tilde{\pi}_2, & \text{если } h(\tilde{1}^n) = 0. \end{cases}$$

Тогда $K_1(\tilde{\rho}) = 1$ и $h(\tilde{\rho}) = \overline{h(\tilde{1}^n)}$. Лемма 1 доказана. ■

Обозначим через $\tilde{\tau}$ двоичный $(n+1)$-разрядный набор, получающийся из набора $\tilde{\rho}$ добавлением справа $(n+1)$-й компоненты, равной единице.

Лемма 2. Любую булеву функцию $f(\tilde{x}^n)$, в представлении (2) которой $m \geqslant 2$, можно реализовать неизбыточной схемой в базисе B, содержащей одну фиктивную входную переменную и допускающей ЕПТ $T = \{(\tilde{0}^r, \tilde{1}^{n+1-r}), (\tilde{1}^s, 0, \tilde{1}^{n-s}), \tilde{\sigma}_{K_1}, \tilde{\tau} \, : \, r \in \{0, \ldots, n+1\}, s \in \{1, \ldots, n\}\}$ (длины не более $2n + 4$).

Доказательство. Представим конъюнкцию K_1 в виде $K_1 \overline{x}_{n+1} \oplus K_1 x_{n+1}$, где x_{n+1} — булева переменная, отличная от $x_1, \ldots, x_n$. Тогда представление (2) примет вид

$$f^{(+1)}(\tilde{x}^{n+1}) = K_1 \overline{x}_{n+1} \oplus K_1 x_{n+1} \oplus K_2 \oplus \ldots \oplus K_m \oplus c.$$

Перепишем последнее равенство в виде

$$f^{(+1)}(\tilde{x}^{n+1}) = K_1 \overline{x}_{n+1} \oplus K_2 \oplus \ldots \oplus K_m \oplus x_{n+1}(K_1 \oplus a) \oplus a x_{n+1} \oplus c. \tag{4}$$

Реализуем функцию $f^{(+1)}$ схемой S в базисе B в соответствии с представлением (4) (см. рис. 1). Каждую конъюнкцию K_i, $i = 1, \ldots, m$, реализуем цепочкой Z_i из $t_i - 1$ конъюнкторов $E_{i,1}, \ldots, E_{i,t_i-1}$, занумерованных «сверху вниз», на входы которой последовательно подаются переменные $x_{j_1(i)}, \ldots, x_{j_{t_i}(i)}$, причём в случае $t_i \geqslant 2$ переменные $x_{j_2(i)}, \ldots, x_{j_{t_i}(i)}$ подаются на правые входы этих конъюнкторов (тогда переменная $x_{j_1(i)}$ будет подана на левый вход элемента $E_{i,1}$ — верхнего конъюнктора цепочки Z_i; в случае $t_i = 1$ в этой цепочке не содержится элементов, а её выход совпадает со входом «$x_{j_1(i)}$» схемы S). Переменную x_{n+1} подадим на вход инвертора I; выход цепочки Z_1 и выход элемента I соединим соответственно с левым и правым входами конъюнктора $E_\&$. Если $a = 1$, то выход цепочки Z_1 соединим также со входом инвертора I'. В случае $a = 0$ выход цепочки Z_1, а в случае $a = 1$ — выход элемента I' соединим с левым входом конъюнктора $E'_\&$, на правый вход которого подадим переменную x_{n+1}. Затем выход элемента $E_\&$, выходы всех цепочек $Z_2, \ldots, Z_m$, выход элемента $E'_\&$ и — в случае $a = 1$ — вход «x_{n+1}» схемы последовательно соединим со входами цепочки $Z_\oplus$, состоящей из сумматоров $E_1^\oplus, \ldots, E_{m+a}^\oplus$, занумерованных «сверху вниз», и — в случае $c = 1$ — из инвертора I'', вход которого соединён с выходом элемента $E_{m+a}^\oplus$, причём выходы цепочек $Z_2, \ldots, Z_m$, выход конъюнктора $E'_\&$ и — в случае $a = 1$ — вход «x_{n+1}» схемы соединим с правыми входами сумматоров $E_1^\oplus, \ldots, E_{m+a}^\oplus$ соответственно (тогда выход конъюнктора $E_\&$ соединяется с левым входом сумматора $E_1^\oplus$). Выход нижнего элемента цепочки $Z_\oplus$ объявим выходом схемы S.

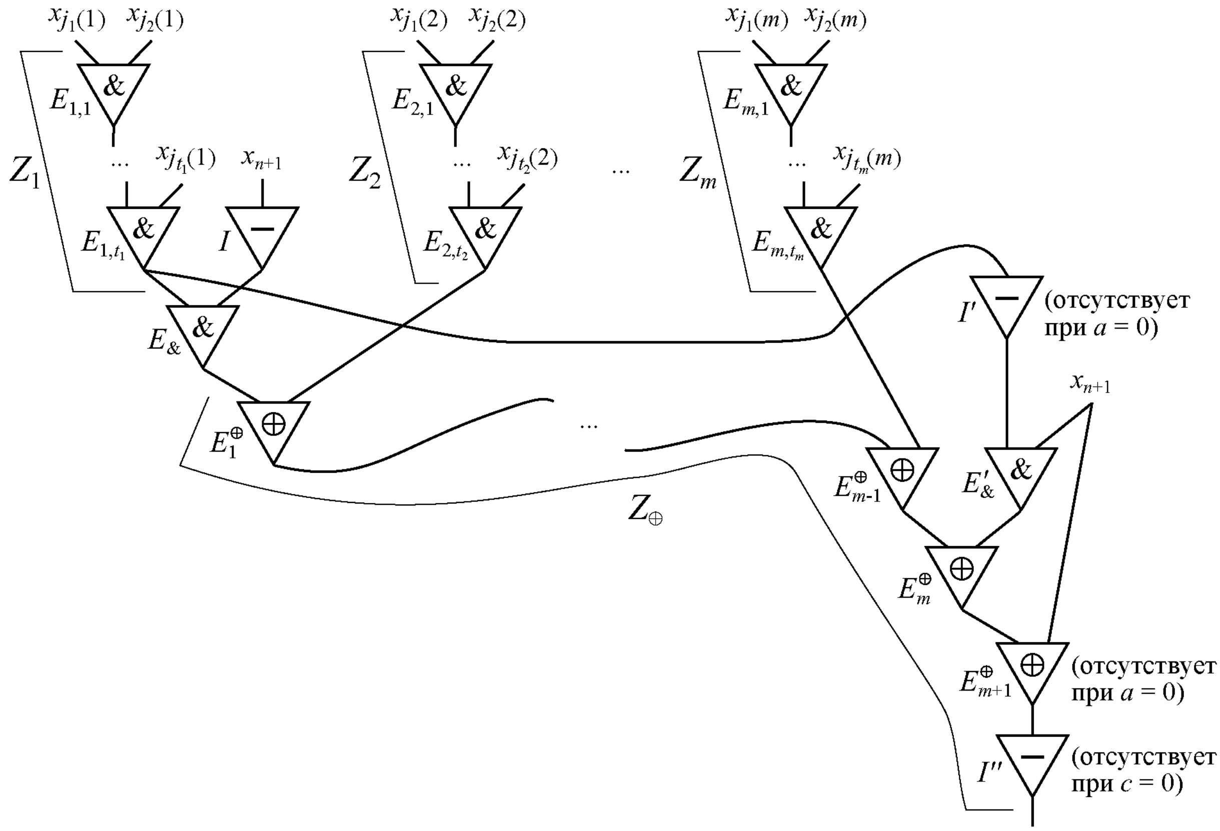

Рис. 1. Схема S

Из построения схемы, представления (4) и тождества (1) вытекает, что схема S при отсутствии в ней неисправностей реализует функцию $f^{(+1)}(\tilde{x}^{n+1})$. Тогда, согласно данному выше определению, схема S содержит одну фиктивную входную переменную и реализует функцию $f(\tilde{x}^n)$. Докажем, что эта схема неизбыточна и допускает ЕПТ T относительно произвольных неисправностей элементов. Достаточно доказать, что любая неисправность любого одного элемента схемы S обнаруживается хотя бы на одном наборе из множества T.

Обозначим через $Z_\oplus^d$, $d = 1, \ldots, m + a + 1$, цепочку, являющуюся нижней частью цепочки $Z_\oplus$ и получающуюся из неё отбрасыванием сумматоров $E_1^\oplus, \ldots, E_{d-1}^\oplus$ (считаем, что в случае $d = 1$ цепочки $Z_\oplus^d$ и $Z_\oplus$ совпадают, а в случае $d = m + a + 1$ и $c = 0$ цепочка $Z_\oplus^d$ не содержит элементов и её выход совпадает с её единственным входом и с выходом элемента $E_{m+a}^\oplus$).

Рассмотрим произвольную неисправность произвольного одного элемента E в схеме S. При этой неисправности на выходе элемента E реализуется булева функция (от его входов), отличающаяся от исходной приписанной ему функции хотя бы на одном наборе $\tilde{\alpha}$; данный набор содержит две компоненты (одну компоненту), если элемент E — конъюнктор или сумматор (соответственно если элемент E — инвертор). Для любого $d \in \{1, \ldots, m + a + 1\}$ цепочка $Z_\oplus^d$ при условии, что в ней не содержится элемента E, очевидно, реализует линейную булеву функцию от своих входов, поэтому изменение значения ровно на одном входе этой цепочки приводит к изменению значения на выходе всей схемы S. Таким образом, если на некотором входном наборе $\tilde{\sigma} \in T$ схемы S при переходе элемента E в неисправное состояние меняется значение ровно на одном входе цепочки $Z_\oplus^d$ для некоторого $d \in \{1, \ldots, m+a+1\}$, не содержащей этого элемента, то указанная неисправность обнаруживается на наборе $\tilde{\sigma}$. Возможны девять случаев:

1. Элемент E — конъюнктор $E_{i,q}$ для некоторых $i \in \{1, \ldots, m\}$, $q \in \{1, \ldots, t_i - 1\}$ (и при этом $t_i \geqslant 2$). В силу построения схемы S на правый вход данного конъюнктора подаётся переменная $x_{j_{q+1}(i)}$, а его левый вход соединяется либо со входом «$x_{j_1(i)}$» схемы (в случае $q = 1$), либо с выходом цепочки из конъюнкторов $E_{i,1}, \ldots, E_{i,q-1}$, на входы которой подаются переменные $x_{j_1(i)}, \ldots, x_{j_q(i)}$ (в случае $q \geqslant 2$); выход элемента $E_{i,q}$ либо является выходом цепочки Z_i (в случае $q = t_i - 1$), либо соединяется с одним из входов цепочки из конъюнкторов $E_{i,q+1}, \ldots, E_{i,t_i-1}$, на другие входы которой подаются переменные $x_{j_{q+2}(i)}, \ldots, x_{j_t(i)}$ и выход которой совпадает с выходом цепочки Z_i (в случае $q \leqslant t_i - 2$). При этом выполнено соотношение (3). Отсюда следует, что при последовательной подаче на входы схемы S наборов

$$(\tilde{0}^{j_{q+1}(i)}, \tilde{1}^{n+1-j_{q+1}(i)}), (\tilde{0}^{j_{q+1}(i)-1}, \tilde{1}^{n+2-j_{q+1}(i)}), (\tilde{1}^{j_{q+1}(i)-1}, 0, \tilde{1}^{n+1-j_{q+1}(i)}), (\tilde{1}^{n+1}) \in T$$

на входах элемента E возникают наборы $(0,0), (0,1), (1,0), (1,1)$ соответственно, а значение на выходе элемента E совпадает со значением на выходе цепочки Z_i (поскольку в случае $q \leqslant t_i - 2$ у каждого из указанных четырёх наборов из множества T все компоненты, начиная с компоненты с номером $j_{q+1}(i) + 1$, равны 1 и $j_{q+1}(i) + 1 \leqslant j_{q+2}(i) < \ldots < j_t(i)$, т. е. на правые входы всех конъюнкторов $E_{i,q+1}, \ldots, E_{i,t_i-1}$ поступают единицы). Значит, существует такой набор $\tilde{\sigma} \in T$, при подаче которого на входы схемы S на входах элемента E возникает набор $\tilde{\alpha}$, а значение на выходе элемента E совпадает со значением на выходе цепочки Z_i, причём $(n+1)$-я (последняя) компонента набора $\tilde{\sigma}$ равна 1, так как $j_{q+1}(i) \leqslant n$. Рассмотрим два подслучая:

1.1. Пусть $i \in \{2, \ldots, m\}$. На входном наборе $\tilde{\sigma}$ схемы S при переходе элемента E в рассматриваемое неисправное состояние меняется значение на выходе цепочки Z_i, а значит, ровно на одном входе цепочки $Z_\oplus^1$, что и требовалось доказать.

1.2. Пусть $i = 1$. Выход цепочки Z_1 в схеме S соединяется с левым входом конъюнктора $E_\&$, а также — непосредственно или через инвертор I' — с левым входом конъюнктора $E'_{\&}$. Правый вход конъюнктора $E_{\&}$ соединяется с выходом инвертора I, и на этом выходе реализуется функция $\overline{x}_{n+1}$, принимающая значение 0 на наборе $\tilde{\sigma}$. Поэтому при подаче на входы схемы S набора $\tilde{\sigma}$ на выходе конъюнктора $E_{\&}$ возникает нуль вне зависимости от значения, возникающего на выходе цепочки Z_1. Далее, на правый вход конъюнктора $E'_{\&}$ подаётся переменная x_{n+1}, равная единице на наборе $\tilde{\sigma}$. Поэтому при подаче на входы схемы S данного набора значение на выходе конъюнктора $E'_{\&}$ в случае $a = 0$ совпадает со значением на выходе цепочки Z_1, а в случае $a = 1$ — со значением на выходе инвертора I' и противоположно значению на выходе цепочки Z_1. В каждом из случаев $a = 0$, $a = 1$ на входном наборе $\tilde{\sigma}$ схемы S при переходе элемента E в рассматриваемое неисправное состояние меняется значение на выходе цепочки Z_1, а значит, и на выходе конъюнктора $E'_{\&}$, т. е. ровно на одном входе цепочки $Z^1_{\oplus}$, что и требовалось доказать.

2. Элемент E — инвертор I. При последовательной подаче на входы схемы S наборов $(\tilde{1}^n, 0), (\tilde{1}^{n+1}) \in T$ на входах элемента E, очевидно, возникают наборы $(0), (1)$ соответственно, а значение на выходе элемента E совпадает со значением на выходе конъюнктора $E_{\&}$ (поскольку на каждом из указанных двух наборов из множества T на выходе цепочки Z_1 возникает значение 1, которое подаётся на левый вход конъюнктора $E_{\&}$). Значит, существует такой набор $\tilde{\sigma} \in T$, при подаче которого на входы схемы S на входах элемента E возникает набор $\tilde{\alpha}$, а значение на выходе элемента E совпадает со значением на выходе конъюнктора $E_{\&}$. Тогда на наборе $\tilde{\sigma}$ при переходе элемента E в рассматриваемое неисправное состояние меняется значение на выходе данного конъюнктора, а значит, ровно на одном входе цепочки $Z^1_{\oplus}$, что и требовалось доказать.

3. Элемент E — инвертор I' (и при этом $a = 1$). При последовательной подаче на входы схемы S наборов $(\tilde{0}^n, 1), (\tilde{1}^{n+1}) \in T$ на входах элемента E, очевидно, возникают наборы $(0), (1)$ соответственно, а значение на выходе элемента E совпадает со значением на выходе конъюнктора $E'_{\&}$ (поскольку на каждом из указанных двух наборов из множества T переменная x_{n+1} принимает значение 1, которое подаётся на правый вход конъюнктора $E'_{\&}$). Значит, существует такой набор $\tilde{\sigma} \in T$, при подаче которого на входы схемы S на входах элемента E возникает набор $\tilde{\alpha}$, а значение на выходе элемента E совпадает со значением на выходе конъюнктора $E'_{\&}$. Тогда на наборе $\tilde{\sigma}$ при переходе элемента E в рассматриваемое неисправное состояние меняется значение на выходе данного конъюнктора, а значит, ровно на одном входе цепочки $Z^1_{\oplus}$, что и требовалось доказать.

4. Элемент E — конъюнктор $E_{\&}$. Легко видеть, что при последовательной подаче на входы схемы S наборов $(\tilde{0}^n, 1), (\tilde{0}^{n+1}), (\tilde{1}^{n+1}), (\tilde{1}^n, 0) \in T$ на входах элемента E возникают наборы $(0, 0), (0, 1), (1, 0), (1, 1)$ соответственно. Значит, существует такой набор $\tilde{\sigma} \in T$, при подаче которого на входы схемы S на входах элемента E возникает набор $\tilde{\alpha}$. Тогда на наборе $\tilde{\sigma}$ при переходе элемента E в рассматриваемое неисправное состояние меняется значение ровно на одном входе цепочки $Z^1_{\oplus}$, что и требовалось доказать.

5. Элемент E — конъюнктор $E'_{\&}$. Легко видеть, что при последовательной подаче на входы схемы S наборов $(\tilde{0}^{n+1}), (\tilde{0}^n, 1), (\tilde{1}^n, 0), (\tilde{1}^{n+1}) \in T$ на входах элемента E возникают наборы $(0, 0), (0, 1), (1, 0), (1, 1)$ соответственно в случае $a = 0$ и наборы $(1, 0), (1, 1), (0, 0), (0, 1)$ — в случае $a = 1$. Значит, существует такой набор $\tilde{\sigma} \in T$, при подаче которого на входы схемы S на входах элемента E возникает набор $\tilde{\alpha}$. Тогда на наборе $\tilde{\sigma}$ при переходе элемента E в рассматриваемое неисправное состояние меняется значение ровно на одном входе цепочки $Z^1_{\oplus}$, что и требовалось доказать.

6. Элемент E — сумматор $E_i^{\oplus}$ для некоторого $i \in \{1, \dots, m-1\}$. Тогда правый вход элемента E по построению схемы S соединён с выходом цепочки Z_{i+1}, на котором реализуется конъюнкция K_{i+1}. При подаче на входы схемы набора $(\tilde{0}^{n+1}) \in T$ на входах элемента E, очевидно, возникает набор $(0, 0)$. При подаче на входы схемы набора $\tilde{\sigma}_{K_1} \in T$ на выходе как цепочки Z_1, так и инвертора I, а значит, и на выходе конъюнктора $E_\&$ возникает значение 1 (см. определение набора $\tilde{\sigma}_{K_1}$; достаточно лишь отметить, что $j_1(1) \leqslant n, \dots, j_{t_1}(1) \leqslant n$), а на выходе каждой из цепочек $Z_2, \dots, Z_m$ — значение 0, поскольку K_1 — самая короткая конъюнкция в полиноме Жегалкина функции $f(\tilde{x}^n)$ и, как следствие, в каждую из конъюнкций $K_2, \dots, K_m$ входит хотя бы одна переменная, отличная от $x_{j_1(1)}, \dots, x_{j_{t_1}(1)}$. Отсюда вытекает, что на наборе $\tilde{\sigma}_{K_1}$ на входах каждого из сумматоров $E_1^{\oplus}, \dots, E_i^{\oplus}$ возникает набор $(1, 0)$. Далее, при последовательной подаче на входы схемы S наборов $(\tilde{1}^n, 0), (\tilde{1}^{n+1}) \in T$ на выходах всех цепочек $Z_1, \dots, Z_m$ возникают единицы, а на выходе инвертора I — значения $1, 0$ соответственно; такие же значения возникают на выходе конъюнктора $E_\&$. Тогда на указанных двух наборах из множества T на входы сумматора $E_1^{\oplus}$ поступают наборы $(1, 1), (0, 1)$ соответственно; в случае $i \geqslant 2$ на выходе этого сумматора возникают значения $0, 1$ соответственно и на входы сумматора $E_2^{\oplus}$ поступают наборы $(0, 1), (1, 1)$; в случае $i \geqslant 3$ на выходе сумматора $E_2^{\oplus}$ возникают значения $1, 0$ соответственно и на входы сумматора $E_3^{\oplus}$ поступают наборы $(1, 1), (0, 1)$, и т. д. В итоге получаем, что на наборах $(\tilde{1}^n, 0), (\tilde{1}^{n+1})$ на входы сумматора $E_i^{\oplus}$, т. е. элемента E, при нечётном i поступают наборы $(1, 1), (0, 1)$ соответственно, а при чётном i — наборы $(0, 1), (1, 1)$ соответственно. С учётом предыдущих рассуждений делаем вывод, что при подаче на входы схемы S некоторых наборов из множества T на входах элемента E возникают все четыре набора $(0, 0), (0, 1), (1, 0), (1, 1)$. Значит, существует такой набор $\tilde{\sigma} \in T$, при подаче которого на входы схемы на входах элемента E возникает набор $\tilde{\alpha}$. Тогда на наборе $\tilde{\sigma}$ при переходе элемента E в рассматриваемое неисправное состояние меняется значение ровно на одном (а именно на левом верхнем) входе цепочки $Z_{\oplus}^{i+1}$, что и требовалось доказать.

7. Элемент E — сумматор $E_m^{\oplus}$. Тогда левый и правый входы элемента E по построению схемы S соединены с выходами элементов $E_{m-1}^{\oplus}$ и $E'_\&$ соответственно и на этих выходах реализуются функции $K_1 \overline{x}_{n+1} \oplus K_2 \oplus \ldots \oplus K_m$ и $x_{n+1}(K_1 \oplus a)$ соответственно. При подаче на входы схемы набора $(\tilde{0}^{n+1}) \in T$ на входах элемента E, очевидно, возникает набор $(0, 0)$. При подаче на входы схемы набора $\tilde{\sigma}_{K_1} \in T$ на правом входе элемента E возникает значение 0, поскольку $(n+1)$-я компонента данного набора равна нулю, а на левом входе — значение $1 \oplus \underbrace{0 \oplus \ldots \oplus 0}_{m-1} = 1$, так как K_1 — самая короткая конъюнкция в полиноме Жегалкина функции $f(\tilde{x}^n)$; следовательно, на входах элемента E возникает набор $(1, 0)$. Докажем, что при подаче на входы схемы S некоторых двух наборов из множества T на входах элемента E возникают наборы $(0, 1)$ и $(1, 1)$. Рассмотрим два подслучая:

7.1. Пусть $a = 1$. На входном наборе $(\tilde{0}^n, 1) \in T$ схемы на входы элемента E поступает набор $(0, 1)$, так как на этом наборе функции $K_1, K_2, \dots, K_m, x_{n+1}, K_1 \oplus a$ (рассматриваемые как функции от переменных $x_1, \dots, x_{n+1}$) принимают значения $\underbrace{0, \dots, 0}_{m}, 1, 1$ соответственно. На входном наборе $\tilde{\tau} \in T$ схемы на входы элемента E поступает набор $(1, 1)$, так как на этом наборе функции $K_1 \overline{x}_{n+1}, K_2 \oplus \ldots \oplus K_m, x_{n+1}, K_1 \oplus a$ принимают значения $0, 1, 1, 1$ соответственно (см. определения наборов $\tilde{\tau}$, $\tilde{\rho}$ и функции $h(\tilde{x}^n)$).

7.2. Пусть $a = 0$. На входном наборе $(\tilde{1}^{n+1}) \in T$ схемы на входы элемента E поступает набор $(h(\tilde{1}^n), 1)$, так как на этом наборе функции $K_1 \overline{x}_{n+1}, K_2 \oplus \ldots \oplus K_m, x_{n+1}, K_1 \oplus a$

принимают значения $0, h(\tilde{1}^n), 1, 1$ соответственно. На входном наборе $\tilde{\tau} \in T$ схемы на входы элемента E поступает набор $\left(\overline{h(\tilde{1}^n)}, 1\right)$, так как на этом наборе функции $K_1\overline{x}_{n+1}, K_2 \oplus \ldots \oplus K_m, x_{n+1}, K_1 \oplus a$ принимают значения $0, \overline{h(\tilde{1}^n)}, 1, 1$ соответственно (см. определения наборов $\tilde{\tau}$ и $\tilde{\rho}$).

В каждом из подслучаев 7.1 и 7.2 доказано, что при подаче на входы схемы S некоторых двух наборов из множества T на входах элемента E возникают наборы $(0,1)$ и $(1,1)$. С учётом предыдущих рассуждений из разбора случая 7 делаем вывод, что при подаче на входы схемы S некоторых наборов из множества T на входах элемента E возникают все четыре набора $(0,0), (0,1), (1,0), (1,1)$. Значит, существует такой набор $\tilde{\sigma} \in T$, при подаче которого на входы схемы на входах элемента E возникает набор $\tilde{\alpha}$. Тогда на наборе $\tilde{\sigma}$ при переходе элемента E в рассматриваемое неисправное состояние меняется значение ровно на одном (а именно на левом верхнем) входе цепочки $Z_{\oplus}^{m+1}$, что и требовалось доказать.

8. Элемент E — сумматор $E_{m+1}^{\oplus}$ (и при этом $a = 1$). Тогда левый и правый входы элемента E по построению схемы S соединены с выходом сумматора $E_m^{\oplus}$ и со входом «x_{n+1}» схемы соответственно и на эти входы элемента E подаются функции $K_1\overline{x}_{n+1} \oplus K_2 \oplus \ldots \oplus K_m \oplus x_{n+1}(K_1 \oplus 1)$ и x_{n+1} соответственно. Используя рассуждения из разбора случая 7 и подслучая 7.1, получаем, что при последовательной подаче на входы схемы S наборов $(\tilde{0}^{n+1}), \tilde{\sigma}_{K_1}, (\tilde{0}^n, 1), \tilde{\tau} \in T$ на входах элемента E возникают наборы $(0 \oplus 0, 0), (1 \oplus 0, 0), (0 \oplus 1, 1), (1 \oplus 1, 1)$ соответственно, т. е. наборы $(0,0), (1,0), (1,1), (0,1)$. Значит, существует такой набор $\tilde{\sigma} \in T$, при подаче которого на входы схемы на входах элемента E возникает набор $\tilde{\alpha}$. Тогда на наборе $\tilde{\sigma}$ при переходе элемента E в рассматриваемое неисправное состояние меняется значение ровно на одном (а именно на левом верхнем) входе цепочки $Z_{\oplus}^{m+2}$, что и требовалось доказать.

9. Элемент E — инвертор I'' (и при этом $c = 1$). Тогда вход элемента E по построению схемы S соединён с выходом сумматора $E_m^{\oplus}$ в случае $a = 0$ и с выходом сумматора $E_{m+1}^{\oplus}$ в случае $a = 1$. Используя рассуждения из разбора случаев 7 и 8, получаем, что в каждом из случаев $a = 0$, $a = 1$ при последовательной подаче на входы схемы S наборов $(\tilde{0}^{n+1}), \tilde{\sigma}_{K_1} \in T$ на входах элемента E возникают наборы $(0 \oplus 0), (1 \oplus 0)$ соответственно, т. е. наборы $(0), (1)$. Значит, существует такой набор $\tilde{\sigma} \in T$, при подаче которого на входы схемы S на входах элемента E возникает набор $\tilde{\alpha}$. Тогда на наборе $\tilde{\sigma}$ при переходе элемента E в рассматриваемое неисправное состояние меняется значение на выходе данного элемента, совпадающем с выходом схемы S, что и требовалось доказать. Лемма 2 доказана. ■

Доказательство теоремы 1. Представим функцию f полиномом Жегалкина (2), где $m \geqslant 1$; $c \in \{0,1\}$; K_1 — самая короткая конъюнкция в этом полиноме. Рассмотрим два случая:

1. Пусть $m = 1$. Реализуем функцию $f^{(+1)}$ схемой S в базисе B в соответствии с представлением $f^{(+1)}(\tilde{x}^{n+1}) = K_1 \oplus c$. Конъюнкцию K_1 реализуем цепочкой Z из $t_1 - 1$ конъюнкторов $E_1, \ldots, E_{t_1-1}$, занумерованных «сверху вниз», на входы которой последовательно подаются переменные $x_{j_1(1)}, \ldots, x_{j_{t_1}(1)}$, причём в случае $t_1 \geqslant 2$ переменные $x_{j_2(1)}, \ldots, x_{j_{t_1}(1)}$ подаются на правые входы этих конъюнкторов (в случае $t_1 = 1$ в цепочке Z не содержится элементов, а её выход совпадает со входом «$x_{j_1(1)}$» схемы S). Если $c = 0$, то выход цепочки Z будем считать выходом схемы S; если $c = 1$, то соединим выход цепочки Z со входом инвертора I, выход которого будем считать выходом схемы S.

Из построения схемы и тождества (1) вытекает, что схема S при отсутствии в ней неисправностей реализует функцию $f^{(+1)}(\tilde{x}^{n+1})$. Тогда схема S содержит одну фиктивную входную переменную и реализует функцию $f(\tilde{x}^n)$. Докажем, что эта схема неизбыточна и допускает ЕПТ $T = \{(\tilde{0}^r, \tilde{1}^{n+1-r}), (\tilde{1}^s, 0, \tilde{1}^{n-s}) : r \in \{0, \ldots, n+1\}, s \in \{1, \ldots, n\}\}$ длины $2n+2$ относительно произвольных неисправностей элементов; отсюда следует справедливость утверждений 1 и 2 теоремы в случае 1. Достаточно доказать, что любая неисправность любого одного элемента схемы S обнаруживается хотя бы на одном наборе из множества T.

Рассмотрим произвольную неисправность произвольного одного элемента E в схеме S. При этой неисправности на выходе элемента E реализуется булева функция (от его входов), отличающаяся от исходной приписанной ему функции хотя бы на одном наборе $\tilde{\alpha}$; данный набор содержит две компоненты (одну компоненту), если элемент E — конъюнктор (соответственно инвертор). Возможны два подслучая:

1.1. Элемент E — конъюнктор E_q для некоторого $q \in \{1, \ldots, t_1-1\}$ (при этом $t_1 \geqslant 2$). Рассуждая по аналогии с разбором случая 1 в доказательстве леммы 2, получаем, что при последовательной подаче на входы схемы S наборов

$$(\tilde{0}^{j_{q+1}(1)}, \tilde{1}^{n+1-j_{q+1}(1)}), (\tilde{0}^{j_{q+1}(1)-1}, \tilde{1}^{n+2-j_{q+1}(1)}), (\tilde{1}^{j_{q+1}(1)-1}, 0, \tilde{1}^{n+1-j_{q+1}(1)}), (\tilde{1}^{n+1}) \in T$$

на входах элемента E возникают наборы $(0,0), (0,1), (1,0), (1,1)$ соответственно, а значение на выходе элемента E совпадает со значением на выходе цепочки Z. Значит, существует такой набор $\tilde{\sigma} \in T$, при подаче которого на входы схемы S на входах элемента E возникает набор $\tilde{\alpha}$, а значение на выходе элемента E совпадает со значением на выходе цепочки Z. На этом наборе при переходе элемента E в рассматриваемое неисправное состояние меняется значение на выходе цепочки Z, а значит, и на выходе схемы S (вне зависимости от того, содержится в ней инвертор I или нет), что и требовалось доказать.

1.2. Элемент E — инвертор I (и при этом $c = 1$). При последовательной подаче на входы схемы S наборов $(\tilde{0}^{n+1}), (\tilde{1}^{n+1}) \in T$ на входах элемента E (число которых равно 1), очевидно, возникают наборы $(0), (1)$ соответственно. Значит, существует такой набор $\tilde{\sigma} \in T$, при подаче которого на входы схемы S на входах элемента E возникает набор $\tilde{\alpha}$. Тогда на наборе $\tilde{\sigma}$ при переходе элемента E в рассматриваемое неисправное состояние меняется значение на выходе данного элемента, совпадающем с выходом схемы S, что и требовалось доказать.

2. Пусть $m \geqslant 2$. Утверждение 1 теоремы 1 сразу следует из леммы 2. Идея доказательства утверждения 2 теоремы состоит в подходящей перенумерации переменных функции $f(\tilde{x}^n)$, при которой набор $\tilde{\tau}$ совпадёт с одним из наборов вида $(\tilde{0}^r, \tilde{1}^{n+1-r})$, где $r \in \{0, \ldots, n\}$. Тогда в описании множества T встретятся два одинаковых набора и верхнюю оценку мощности этого множества, т. е. длины теста, можно будет понизить с $2n+4$ до $2n+3$.

Пусть набор $\tilde{\rho}$ для функции $f(\tilde{x}^n)$, удовлетворяющий условию леммы 1, равен $(\rho_1, \ldots, \rho_n)$ и имеет u нулевых и $n-u$ единичных компонент, причём в случае $u \geqslant 1$ номера его нулевых компонент равны $i_1, \ldots, i_u$, где $i_1 < \ldots < i_u$, а в случае $u \leqslant n-1$ номера его единичных компонент равны $i_{u+1}, \ldots, i_n$, где $i_{u+1} < \ldots < i_n$. Тогда $i_1, \ldots, i_n$ — попарно различные индексы от 1 до n, поэтому существуют такие индексы $i'_1, \ldots, i'_n$ от 1 до n, что $i_{i'_1} = 1, \ldots, i_{i'_n} = n$. Положим $f'(\tilde{x}^n) = f(x_{i'_1}, \ldots, x_{i'_n})$, $K'_1(\tilde{x}^n) = K_1(x_{i'_1}, \ldots, x_{i'_n}), \ldots, K'_m(\tilde{x}^n) = K_m(x_{i'_1}, \ldots, x_{i'_n})$. Пусть $\varphi(\tilde{x}^n)$ — произвольная булева функция и $\varphi'(\tilde{x}^n) = \varphi(x_{i'_1}, \ldots, x_{i'_n})$. Имеем

$$\varphi'(x_{i_1}, \ldots, x_{i_n}) = \varphi(x_{i_{i'_1}}, \ldots, x_{i_{i'_n}}) = \varphi(\tilde{x}^n), \qquad (5)$$

$$f'(\tilde{x}^n) = f(x_{i'_1}, \ldots, x_{i'_n}) = K_1(x_{i'_1}, \ldots, x_{i'_n}) \oplus \ldots \oplus K_m(x_{i'_1}, \ldots, x_{i'_n}) \oplus c = \\ = K'_1(\tilde{x}^n) \oplus \ldots \oplus K'_m(\tilde{x}^n) \oplus c,$$

т. е.

$$f'(\tilde{x}^n) = K'_1 \oplus \ldots \oplus K'_m \oplus c.$$

Последнее равенство задаёт представление булевой функции $f'(\tilde{x}^n)$ полиномом Жегалкина, причём K'_1 — самая короткая конъюнкция в этом полиноме, поскольку ранги конъюнкций $K'_1, \ldots, K'_m$ совпадают с рангами конъюнкций $K_1, \ldots, K_m$ соответственно. Пусть $h'(\tilde{x}^n) = K'_2 \oplus \ldots \oplus K'_m$,

$$a' = \begin{cases} 1, & \text{если } K'_1 \leqslant h' \text{ или } K'_1 \leqslant h' \oplus 1, \\ 0 & \text{иначе.} \end{cases}$$

Тогда

$$h'(\tilde{x}^n) = K_2(x_{i'_1}, \ldots, x_{i'_n}) \oplus \ldots \oplus K_m(x_{i'_1}, \ldots, x_{i'_n}) = h(x_{i'_1}, \ldots, x_{i'_n}).$$

Отсюда и из определения функции $K_1(\tilde{x}^n)$ следует, что неравенство $K'_1 \leqslant h'$ равносильно неравенству $K_1 \leqslant h$, а неравенство $K'_1 \leqslant h' \oplus 1$ — неравенству $K_1 \leqslant h \oplus 1$. Таким образом, $a' = a$. Далее, пусть $\tilde{\sigma}_{K'_1}$ — двоичный $(n+1)$-разрядный набор, содержащий единицы только в тех компонентах, которые отвечают переменным, входящим в конъюнкцию K'_1, а $\tilde{\rho}' = (\tilde{0}^u, \tilde{1}^{n-u})$. В силу определения набора $\tilde{\rho}$ в случае $a = 1$ выполнены равенства $K_1(\tilde{\rho}) = 0$ и $h(\tilde{\rho}) = 1$, а в случае $a = 0$ — равенства $K_1(\tilde{\rho}) = 1$ и $h(\tilde{\rho}) = \overline{h(\tilde{1}^n)}$. Тогда в случае $a' = 1$, т. е. $a = 1$, в силу (5) выполнены равенства

$$0 = K_1(\tilde{\rho}) = K'_1(\rho_{i_1}, \ldots, \rho_{i_u}, \rho_{i_{u+1}}, \ldots, \rho_{i_n}) = K'_1(\tilde{0}^u, \tilde{1}^{n-u}) = K'_1(\tilde{\rho}')$$

и, аналогично, $1 = h(\tilde{\rho}) = h'(\tilde{\rho}')$, а в случае $a' = 0$, т. е. $a = 0$ — равенства $1 = K_1(\tilde{\rho}) = K'_1(\tilde{\rho}')$, $h(\tilde{\rho}) = h'(\tilde{\rho}')$ и $h(\tilde{1}^n) = h'(\tilde{1}^n)$ (набор $(\tilde{1}^n)$ не меняется при перестановке его компонент), откуда $h'(\tilde{\rho}') = \overline{h'(\tilde{1}^n)}$. Обозначим через $\tilde{\tau}'$ двоичный $(n+1)$-разрядный набор, получающийся из набора $\tilde{\rho}'$ добавлением справа $(n+1)$-й компоненты, равной единице. Тогда $\tilde{\tau}' = (\tilde{0}^u, \tilde{1}^{n-u+1})$. В силу леммы 2 (в исходных обозначениях которой к $f, K_1, \ldots, K_m, h, a, \tilde{\rho}, \tilde{\tau}$ добавлены штрихи) функцию $f'(\tilde{x}^n)$ можно реализовать неизбыточной схемой S' в базисе B, содержащей одну фиктивную входную переменную и допускающей ЕПТ $T' = \{(\tilde{0}^r, \tilde{1}^{n+1-r}), (\tilde{1}^s, 0, \tilde{1}^{n-s}), \tilde{\sigma}_{K'_1}, \tilde{\tau}' : r \in \{0, \ldots, n+1\}, s \in \{1, \ldots, n\}\}$. Заметим, что $\tilde{\tau}' = (\tilde{0}^r, \tilde{1}^{n+1-r})$ при $r = u$, поэтому мощность множества T' не превосходит $2n + 3$. Схема S', согласно определению, реализует булеву функцию $f'^{(+1)}(\tilde{x}^{n+1})$, не зависящую существенно от переменной x_{n+1} и равную функции $f'(\tilde{x}^n)$, т. е. функции $f(x_{i'_1}, \ldots, x_{i'_n})$. Тогда $f'^{(+1)}(\tilde{x}^{n+1}) = f^{(+1)}(x_{i'_1}, \ldots, x_{i'_n}, x_{n+1})$. Нетрудно показать, что если на входы схемы S' вместо переменных $x_{i'_1}, \ldots, x_{i'_n}, x_{n+1}$ подать переменные $x_1, \ldots, x_n, x_{n+1}$ соответственно, то полученная СФЭ в базисе B реализует функцию $f^{(+1)}(\tilde{x}^{n+1})$ (а значит, содержит одну фиктивную входную переменную и реализует функцию $f(\tilde{x}^n)$), неизбыточна и допускает ЕПТ длины не более $2n + 3$, получающийся из множества T' перестановкой компонент каждого набора, содержащегося в T', при которой i'_1-я, …, i'_n-я, $(n+1)$-я компоненты становятся 1-й, …, n-й, $(n+1)$-й компонентами. Утверждение 2 теоремы 1 в случае 2, а вместе с ним и вся теорема 1 доказаны. ■

Заключение

В работе предложен метод реализации любой неконстантной булевой функции $f(\tilde{x}^n)$ схемой из функциональных элементов в базисе $\{\&, \oplus, \neg\}$, содержащей одну фиктивную входную переменную, неизбыточной и допускающей единичный проверяющий тест длины не более $2n+3$ относительно произвольных неисправностей элементов, существенно более короткий, чем тривиальный тест из 2^{n+1} наборов. Данный метод может быть использован на практике для построения легкотестируемых интегральных схем в случае, когда тип допустимых неисправностей содержащихся в них элементов никак не ограничивается (в частности, не ограничивается хорошо изученными константными либо инверсными неисправностями на входах и/или выходах элементов).

Следующим шагом, по мнению автора, должно стать получение линейной по n верхней оценки длины единичного проверяющего теста для неизбыточных схем из функциональных элементов в том же базисе, реализующих произвольные неконстантные булевы функции от n переменных и не содержащих фиктивных переменных (в предположении, что рассматриваются произвольные неисправности элементов). У автора имеется задел в этом направлении.

ЛИТЕРАТУРА

1. *Чегис И. А., Яблонский С. В.* Логические способы контроля работы электрических схем // Труды МИАН. 1958. Т. 51. С. 270–360.
2. *Яблонский С. В.* Надёжность и контроль управляющих систем // Материалы Всесоюзного семинара по дискретной математике и её приложениям (Москва, 31 января–2 февраля 1984 г.). М.: Изд-во МГУ, 1986. С. 7–12.
3. *Яблонский С. В.* Некоторые вопросы надёжности и контроля управляющих систем // Математические вопросы кибернетики. Вып. 1. М.: Наука, 1988. С. 5–25.
4. *Редькин Н. П.* Надёжность и диагностика схем. М.: Изд-во МГУ, 1992. 192 с.
5. *Бородина Ю. В.* О схемах, допускающих единичные тесты длины 1 при константных неисправностях на выходах элементов // Вестник Московского университета. Сер. 1. Математика. Механика. 2008. № 5. С. 49–52.
6. *Попков К. А.* Нижние оценки длин единичных тестов для схем из функциональных элементов // Дискретная математика. 2017. Т. 29. Вып. 2. С. 53–69.
7. *Попков К. А.* Единичные проверяющие тесты для схем из функциональных элементов в базисе «конъюнкция-отрицание» // Прикладная дискретная математика. 2017. № 38. С. 66–88.
8. *Reddy S. M.* Easily testable realizations for logic functions // IEEE Trans. Comput. 1972. V. C-21. Iss. 11. P. 1183–1188.
9. *Коляда С. С.* Единичные проверяющие тесты для схем из функциональных элементов // Вестник Московского университета. Сер. 1. Математика. Механика. 2013. № 4. С. 32–34.
10. *Коляда С. С.* Верхние оценки длины проверяющих тестов для схем из функциональных элементов: дис. … канд. физ.-мат. наук. М., 2013. 77 с.
11. *Романов Д. С.* Метод синтеза легкотестируемых схем, допускающих единичные проверяющие тесты константной длины // Дискретная математика. 2014. Т. 26. Вып. 2. С. 100–130.
12. *Романов Д. С.* О тестах для схем при неисправностях на выходах элементов // Материалы XVIII Междунар. конф. «Проблемы теоретической кибернетики» (Пенза, 19–23 июня 2017 г.). М.: МАКС Пресс, 2017. С. 213–216.

13. *Попков К. А.* Короткие единичные тесты для схем при произвольных константных неисправностях на выходах элементов // Дискретная математика. 2018. Т. 30. Вып. 3. С. 99–116.
14. *Коваценко С. В.* Синтез легкотестируемых схем в базисе Жегалкина для инверсных неисправностей // Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика. 2000. № 2. С. 45–47.
15. *Редькин Н. П.* О единичных проверяющих тестах схем при инверсных неисправностях элементов // XII Междунар. конф. по проблемам теоретической кибернетики (Н. Новгород, 1999). Тез. докл. М.: Изд-во механико-математического факультета МГУ, 1999. С. 196.
16. *Редькин Н. П.* Единичные проверяющие тесты для схем при инверсных неисправностях элементов // Математические вопросы кибернетики. Вып. 12. М.: Физматлит, 2003. С. 217–230.
17. *Попков К. А.* Синтез легкотестируемых схем при однотипных константных неисправностях на входах и выходах элементов // Интеллектуальные системы. Теория и приложения. 2018. Т. 23. Вып. 3. С. 131–147.
18. *Романов Д. С., Романова Е. Ю.* Короткие тесты для схем в базисе Жегалкина // Интеллектуальные системы. Теория и приложения. 2016. Т. 20. Вып. 3. С. 73–78.
19. *Романов Д. С., Романова Е. Ю.* Метод синтеза неизбыточных схем, допускающих единичные проверяющие тесты константной длины // Дискретная математика. 2017. Т. 29. Вып. 4. С. 87–105.
20. *Попков К. А.* Синтез легкотестируемых схем при произвольных константных неисправностях на входах и выходах элементов // Прикладная дискретная математика. 2019. № 43. С. 78–100.
21. *Попков К. А.* Метод построения легко диагностируемых схем из функциональных элементов относительно единичных неисправностей // Прикладная дискретная математика. 2019. № 46. С. 38–57.
22. *Попков К. А.* Короткие полные проверяющие тесты для схем из двухвходовых функциональных элементов // Дискретный анализ и исследование операций. 2019. Т. 26. № 1. С. 89–113.
23. *Яблонский С. В.* Введение в дискретную математику. М.: Наука, 1986. 384 с.

REFERENCES

1. *Chegis I. A. and Yablonskiy S. V.* Logicheskie sposoby kontrolya raboty elektricheskikh skhem [Logical methods of control of work of electric circuits]. Trudy Mat. Inst. Steklov, 1958, vol. 51, pp. 270–360. (in Russian)
2. *Yablonskiy S. V.* Nadezhnost' i kontrol' upravlyayushchikh sistem [Reliability and verification of control systems]. Materialy Vsesoyuznogo seminara po diskretnoy matematike i ee prilozheniyam (Moscow, 31 Jan.–2 Feb. 1984). Moscow., MSU Publ., 1986, pp. 7–12. (in Russian)
3. *Yablonskiy S. V.* Nekotorye voprosy nadezhnosti i kontrolya upravlyayushchikh sistem [Some questions of reliability and verification of control systems]. Matematicheskie Voprosy Kibernetiki, iss. 1, Moscow, Nauka Publ., 1988, pp. 5–25. (in Russian)
4. *Red'kin N. P.* Nadezhnost' i diagnostika skhem [Circuits Reliability and Diagnostics]. Moscow, MSU Publ., 1992. 192 p. (in Russian)
5. *Borodina Yu. V.* Circuits admitting single-fault tests of length 1 under constant faults at outputs of elements. Mosc. Univ. Math. Bull., 2008, vol. 63, iss. 5, pp. 202–204.
6. *Popkov K. A.* Lower bounds for lengths of single tests for Boolean circuits. Discrete Math. Appl., 2019, vol. 29, iss. 1, pp. 23–33.

7. *Popkov K. A.* Edinichnye proveryayushchie testy dlya skhem iz funktsional'nykh elementov v bazise "kon'yunktsiya-otritsanie" [Single fault detection tests for logic networks in the basis "conjunction-negation"]. Prikladnaya Diskretnaya Matematika, 2017, no. 38, pp. 66–88. (in Russian)
8. *Reddy S. M.* Easily testable realizations for logic functions. IEEE Trans. Comput., 1972, vol. C-21, iss. 11, pp. 1183–1188.
9. *Kolyada S. S.* Single fault detection tests for circuits of functional elements. Mosc. Univ. Math. Bull., 2013, vol. 68, iss. 4, pp. 192–193.
10. *Kolyada S. S.* Verkhnie otsenki dliny proveryayushchikh testov dlya skhem iz funktsional'nykh elementov [Upper bounds on length of fault detection tests for logic networks]. Cand. Diss., Moscow, 2013. 77 p. (in Russian)
11. *Romanov D. S.* Method of synthesis of easily testable circuits admitting single fault detection tests of constant length. Discrete Math. Appl., 2014, vol. 24, iss. 4, pp. 227–251.
12. *Romanov D. S.* O testakh dlya skhem pri neispravnostyakh na vykhodakh elementov [On tests for logic networks under faults at outputs of gates]. Materialy XVIII Mezhdunarodnoy konferentsii "Problemy teoreticheskoy kibernetiki" (Penza, 19–23 June 2017). Moscow, MAKS Press Publ., 2017, pp. 213–216. (in Russian)
13. *Popkov K. A.* Short single tests for circuits with arbitrary stuck-at faults at outputs of gates. Discrete Math. Appl., 2019, vol. 29, iss. 5, pp. 321–333.
14. *Kovatsenko S. V.* Sintez legkotestiruemykh skhem v bazise Zhegalkina dlya inversnykh neispravnostey [Synthesis of easily testable logic networks in the Zhegalkin basis for inverse faults]. Vestnik MSU, Ser. 15, 2000, no. 2, pp. 45–47. (in Russian)
15. *Red'kin N. P.* O edinichnykh proveryayushchikh testakh skhem pri inversnykh neispravnostyakh elementov [On single fault detection tests of logic networks under inverse faults of gates]. XII Mezhdunarodnaya konferentsiya po problemam teoreticheskoy kibernetiki (Nizhny Novgorod, 1999). Tezisy dokladov, Moscow, Mech.-Math. Faculty of MSU Publ., 1999, p. 196. (in Russian)
16. *Red'kin N. P.* Edinichnye proveryayushchie testy dlya skhem pri inversnykh neispravnostyakh elementov [Single fault detection tests for logic networks under inverse faults of gates]. Matematicheskie Voprosy Kibernetiki, iss. 12, Moscow, Fizmatlit Publ., 2003, pp. 217–230. (in Russian)
17. *Popkov K. A.* Sintez legkotestiruemykh skhem pri odnotipnykh konstantnykh neispravnostyakh na vkhodakh i vykhodakh elementov [Synthesis of easily testable logic networks under one-type stuck-at faults at inputs and outputs of gates]. Intellektual'nye Sistemy. Teoriya i Prilozheniya, 2018, vol. 23, iss. 3, pp. 131–147. (in Russian)
18. *Romanov D. S., Romanova E. Yu.* Korotkie testy dlya skhem v bazise Zhegalkina [Short tests for circuits in the Zhegalkin basis]. Intellektual'nye Sistemy. Teoriya i Prilozheniya, 2016, vol. 20, iss. 3, pp. 73–78. (in Russian)
19. *Romanov D. S., Romanova E. Yu.* A method of synthesis of irredundant circuits admitting single fault detection tests of constant length. Discrete Math. Appl., 2019, vol. 29, iss. 1, pp. 35–48.
20. *Popkov K. A.* Sintez legkotestiruemykh skhem pri proizvol'nykh konstantnykh neispravnostyakh na vkhodakh i vykhodakh elementov [Synthesis of easily testable logic networks under arbitrary stuck-at faults at inputs and outputs of gates]. Prikladnaya Diskretnaya Matematika, 2019, no. 43, pp. 78–100. (in Russian)
21. *Popkov K. A.* Metod postroeniya legko diagnostiruemykh skhem iz funktsional'nykh elementov otnositel'no edinichnykh neispravnostey [A method of constructing of easily diagnosable logic networks regarding single faults]. Prikladnaya Diskretnaya Matematika, 2019, no. 46, pp. 38–57. (in Russian)

22. *Popkov K. A.* Short complete fault detection tests for logic networks with fan-in two. Journ. Appl. Industr. Math., 2019, vol. 13, iss. 1, pp. 118–131.
23. *Yablonskiy S. V.* Vvedenie v diskretnuyu matematiku [Introduction to Discrete Mathematics]. Moscow, Nauka Publ., 1986. 384 p. (in Russian)