ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь—февраль 2015. Том 22, № 1. С. 51–63

УДК 519.718

ПРОВЕРЯЮЩИЕ ТЕСТЫ ДЛЯ БУЛЕВЫХ ФУНКЦИЙ ПРИ ЛИНЕЙНЫХ ЛОКАЛЬНЫХ НЕИСПРАВНОСТЯХ ВХОДОВ СХЕМ *)

Е. В. Морозов[1], *Д. С. Романов*[1]
[1]Московский гос. университет им. М. В. Ломоносова,
ул. Ленинские горы, 1, 119992 Москва, Россия
e-mail: morozov_msu@mail.ru, romanov@cs.msu.ru

Аннотация. Под линейным локальным k-кратным слипанием переменных понимается подстановка вместо данных переменных линейной булевой функции, зависящей от них. В настоящей работе изучаются проверяющие тесты относительно подобных неисправностей. Известные ранее результаты в двух случаях доводятся до асимптотики, в третьем случае находится порядковая оценка. Библиогр. 5.

Ключевые слова: тест, булева функция, слипание.

Введение

Пусть Φ — множество булевых функций такое, что для любого $m \in \mathbb{N}$ существует $\varphi(y_1, \ldots, y_m) \in \Phi$. Будем говорить, что в булевой функции $f(x_1, \ldots, x_n)$ произошло *локальное k-кратное Φ-слипание* переменных $x_i, \ldots, x_{i+k-1}$, если вместо исходной функции реализуется булева функция, полученная из неё подстановкой вместо каждой из переменных $x_i, \ldots, x_{i+k-1}$ функции $\varphi(x_i, \ldots, x_{i+k-1}) \in \Phi$ (φ будем также называть *функцией слипания*).

Пусть натуральные числа $p, i_1, \ldots, i_p$ таковы, что $1 \leqslant i_1 < i_1 + k - 1 < i_2 < i_2 + k - 1 < \cdots < i_p < i_p + k - 1 \leqslant n$. Будем говорить, что в булевой функции $f(x_1, \ldots, x_n)$ произошло *множественное локальное k-кратное Φ-слипание* переменных $x_{i_1}, \ldots, x_{i_1+k-1}, \ldots, x_{i_p}, \ldots, x_{i_p+k-1}$, если вместо исходной функции реализуется булева функция, полученная из неё подстановкой вместо каждой из переменных $x_{i_j}, \ldots, x_{i_j+k-1}$,

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 12–01–00964-а, 13–01–00958-а и 15–01–07474-а).

$j \in [1,p]$, функции $\varphi_j(x_{i_j},\dots,x_{i_j+k-1})$. Пусть $\Psi_{f,\Phi}^{\text{single}}$ ($\Psi_{f,\Phi}^{\text{multiple}}$) — множество функций неисправности, получающихся из функции f в результате всевозможных (множественных) локальных k-кратных Ф-слипаний переменных (при любых допустимых $p, i_1,\dots,i_p,\varphi_1,\dots,\varphi_p$). Множество наборов T называется *единичным* (*полным*) *проверяющим тестом относительно локальных k-кратных Ф-слипаний переменных*, если для любой функции $g(x_1,\dots,x_n) \in \Psi_{f,\Phi}^{\text{single}}$ ($g(x_1,\dots,x_n) \in \Psi_{f,\Phi}^{\text{multiple}}$), не равной тождественно $f(x_1,\dots,x_n)$, в T найдётся набор, на котором эта функция принимает разные значения. Все результаты данной работы справедливы как для единичных, так и для полных тестов, поэтому далее эти термины будем опускать. *Длиной теста T* назовём число наборов в нём. Тест минимальной длины называется *минимальным*. *Функцией Шеннона* $L(n,k) = L(n,k,\Phi)$ длины проверяющего теста называется максимум по всем булевым функциям n переменных длины минимального проверяющего теста относительно локальных k-кратных Ф-слипаний. Введём аналогично величину $L^*(n,k) = L^*(n,k,\Phi)$, рассматривая максимум по булевым функциям n переменных, существенно зависящим от всех своих переменных. В данной работе изучается случай, когда Ф-слипания являются линейными слипаниями, т. е. Ф — множество всех линейных функций.

Помимо проверяющих тестов существуют также диагностические тесты, цель которых — определить реализовавшуюся функцию неисправности. В [1, 5] изучались проверяющие и диагностические тесты относительно локальных k-кратных Ф-слипаний, когда Ф — множество всех булевых функций. Источник неисправностей, связанный с линейными локальными k-кратными Ф-слипаниями, рассматривался в [3]. При некоторых условиях получена асимптотика функции Шеннона длины диагностического теста и установлен линейный порядок величин $L(n,k)$ и $L^*(n,k)$. Однако неверно рассчитана нижняя оценка этих величин. В доказательстве неявно предполагалось, что отличить конъюнкцию m переменных от множества всех линейных функций m переменных можно, используя тест длиной не менее чем $m+1$, что неверно, так как достаточно четырёх наборов, как будет показано далее. В настоящей работе получены уточнённые верхние и нижние оценки величин $L(n,k,\Phi)$, $L^*(n,k,\Phi)$ при определённых условиях.

1. Вспомогательные определения и леммы

Проверяющей парой для переменных x_i, x_j, $i \neq j$, функции $f(x_1,\dots,x_n)$ назовём пару наборов $\widetilde{\alpha} = (\alpha_1,\dots,\alpha_n)$, $\widetilde{\beta} = (\beta_1,\dots,\beta_n)$ таких, что

$f(\widetilde{\alpha}) \neq f(\widetilde{\beta})$, $\alpha_k \neq \beta_k$ при $k \in \{i, j\}$ и $\alpha_k = \beta_k$ при всех остальных k.

Ребром направления x_i для функции $f(x_1, \ldots, x_n)$ назовём пару наборов, соседних по x_i. Если на них функция принимает разные значения, то ребро называется *правильным*.

Нетрудно видеть, что можно найти набор и добавить его к проверяющей паре для x_i, x_j такой, что среди данных трёх наборов содержалось бы правильное ребро направления x_i или x_j. Если обе переменные существенны, то, добавив к ним правильное ребро направления оставшейся переменной, получим *проверяющую пятёрку*.

Введём бинарное отношение R_f на множестве переменных функции $f(\widetilde{x}^n)$. Всегда верно, что $x_i R_f x_i$. Если $i \neq j$, то $x_i R_f x_j$ тогда и только тогда, когда для переменных x_i, x_j функции $f(\widetilde{x}^n)$ не существует проверяющей пары. В [2] установлено, что R_f — отношение эквивалентности. Следовательно, множество переменных $x_1, \ldots, x_n$ разбивается на непересекающиеся классы эквивалентности по данному отношению. Каждый такой класс назовём *множеством линейности*.

Множество подряд идущих переменных $x_i, \ldots, x_{i+p}$ будем называть *линейно-фиктивно нерасширяемым*, если существенные переменные из этого множества принадлежат одному множеству линейности, а при добавлении к ним x_{i-1} или x_{i+p+1} это свойство не будет выполняться. Если у функции $f(x_1, \ldots, x_n)$ все переменные существенны, то линейно-фиктивно нерасширяемое множество будем для простоты называть *линейно нерасширяемым* множеством.

Проверяющим множеством $S_k(f)$ для функции $f(x_1, \ldots, x_n)$ назовём множество наборов такое, что если при любом допустимом i переменные $x_i, \ldots, x_{i+k-1}$ не лежат внутри одного линейно-фиктивно нерасширяемого множества, то для каких-то существенных переменных среди $x_i, \ldots, x_{i+k-1}$ в $S_k(f)$ имеется проверяющая пятёрка.

Лемма 1. *При $n \to \infty$, $k \to \infty$ для функции $f(x_1, \ldots, x_n)$ можно построить проверяющее множество $S_k(f)$ мощностью асимптотически не более $15\frac{n}{k}$. Если же $f(x_1, \ldots, n)$ существенно зависит от всех своих переменных, то можно построить $S_k(f)$ мощностью асимптотически не более $10\frac{n}{k}$.*

Доказательство. Будем формировать множество $S_k(f)$.

Пусть $i_1 \geqslant 1$ — наименьшее число такое, что $x_{i_1}, \ldots, x_{i_1+k-1}$ не лежат в одном линейно-фиктивно нерасширяемом множестве. Выберем максимальные p_1, q_1 такие, что $i_1 \leqslant p_1 < q_1 \leqslant i_1 + k - 1$ и для переменных x_{p_1}, x_{q_1} существует проверяющая пара. Добавим для них проверяющую пару в $S_k(f)$. Выберем $i_2 \geqslant p_1 + 1$ — наименьшее число

такое, что $x_{i_2}, \ldots, x_{i_2+k-1}$ не лежат в одном линейно-фиктивно нерасширяемом множестве (при меньших i_2 проверяющая пара для каких-то переменных из $x_{i_2}, \ldots, x_{i_2+k-1}$ либо уже лежит в $S_k(f)$, либо все эти переменные лежат внутри линейно-фиктивно нерасширяемого множества). Выбираем p_2, q_2 тем же способом, что выбирались p_1, q_1, тогда $i_2 \leqslant p_2 < q_2 \leqslant i_2 + k - 1$. Заметим также, что $q_2 > i_1 + k - 1$. Действительно, иначе на предыдущем шаге вместо p_1 следовало бы взять p_2, и тогда p_1 не было бы максимальным числом с указанными выше свойствами. Добавляем проверяющую пару для x_{p_2}, x_{q_2}. Переходим к следующем шагу, на котором $i_3 \geqslant p_2 + 1$, а $q_3 > i_2 + k - 1$. Аналогично при меньших значениях i_3 переменные либо лежат внутри линейно-фиктивно нерасширяемого множества, либо проверяющая пара для каких-то двух из этих переменных уже добавлена, и т. д. Получаем, что на j-м шаге добавляется проверяющая пара для некоторых переменных из множества $x_{i_j}, \ldots, x_{i_j+k-1}$, при этом $i_j \geqslant p_{j-1} + 1$, $q_j > i_{j-1} + k - 1$. Покажем также, что $p_j \geqslant q_{j-1}$. Пусть это не так, т. е. $p_j < q_{j-1}$. Поскольку $p_j > p_{j-1}$, в этом случае x_{p_j} либо фиктивна, либо лежит в одном множестве линейности с $x_{q_{j-1}}$. Первого случая не может быть по определению p_j. Если верен второй случай, то для переменных $x_{q_{j-1}}, x_{q_j}$ существует проверяющая пара, что противоречит максимальности p_j. Поэтому $p_j \geqslant q_{j-1}$. Таким образом, получаем цепочку неравенств:

$$q_j > i_{j-1} + k - 1 \geqslant p_{j-2} + k \geqslant q_{j-3} + k.$$

Тем самым при указанных условиях на n и k число пар переменных, для которых добавлена проверяющая пара, асимптотически не больше чем $3\frac{n}{k}$. По построению получается, что среди каждых k-подряд идущих переменных, не принадлежащих одному линейно-фиктивно нерасширяемому множеству, найдётся две переменные, для которых в $S_k(f)$ была добавлена проверяющая пара. Добавим для каждой пары три набора так, чтобы получалась проверяющая пятёрка. Тогда $|S_k(f)| \lesssim 15\frac{n}{k}$.

Пусть $f(x_1, \ldots, x_n)$ существенно зависит от всех своих переменных. Заметим, что в этом случае $q_j = i_j + k - 1$. Действительно, пусть среди переменных $x_{i_j}, \ldots, x_{i_j+k-1}$ не все переменные принадлежат одному множеству линейности. Тогда существует переменная x_{i_j+t}, $t < k - 1$, для которой есть проверяющая пара с переменной x_{i_j+k-1}. Выберем t максимально возможным. Все переменные $x_{i_j+t+1}, \ldots, x_{i_j+k-1}$ принадлежат одному множеству линейности. Тогда $p_j = i_j + t$, $q_j = i_j + k - 1$, поэтому неравенства из предыдущего абзаца преобразуются в следующие:

$i_j \geqslant p_{j-1} + 1$, $p_j \geqslant q_{j-1}$, $q_j = i_j + k - 1$. Получаем

$$q_j = i_j + k - 1 \geqslant p_{j-1} + k \geqslant q_{j-2} + k.$$

Тогда при указанных условиях на n и k число пар переменных, для которых добавлена проверяющая пара, асимптотически не больше чем $2\frac{n}{k}$. Строим по ним $S_k(f)$, $|S_k(f)| \lesssim 10\frac{n}{k}$. Лемма 1 доказана.

Лемма 2. *Пусть все переменные функции $t(x_1, \ldots, x_m)$ принадлежат одному множеству линейности. Тогда $t(x_1, \ldots, x_m)$ — одна из четырёх функций:* $0,\ 1,\ x_1 \oplus x_2 \oplus \cdots \oplus x_m,\ x_1 \oplus x_2 \oplus \cdots \oplus x_m \oplus 1$.

Доказательство. Наборы проверяющей пары отличаются в двух разрядах. Следовательно, если взять произвольный набор $\widetilde{\alpha}$, у которого в i-й позиции стоит нуль, а в j-й позиции стоит единица, и набор $\widetilde{\beta}$, отличающийся от него ровно в этих разрядах, значения функции на данных наборах будут одинаковы. Получаем, что $t(x_1, \ldots, x_m)$ — симметрическая функция. Кроме того, если в произвольном наборе $\widetilde{\gamma}$ в позициях i и j стоят нули, а набор $\widetilde{\delta}$ отличается от него ровно в этих двух разрядах, то значения функции на данных наборах также будут одинаковы. Следовательно, функция $t(x_1, \ldots, x_m)$ на всех чётных слоях булева куба принимает некоторое значение a, а на всех нечётных — некоторое значение b. Таких функций всего четыре: $0,\ 1,\ x_1 \oplus x_2 \oplus \cdots \oplus x_m,\ x_1 \oplus x_2 \oplus \cdots \oplus x_m \oplus 1$. Лемма 2 доказана.

Лемма 3. *Пусть $g(x_1, \ldots, x_m)$ — линейная функция m переменных, $A = \{\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_m\}$ — множество булевых наборов. Тогда существует отличная от g линейная функция $h(x_1, \ldots, x_m)$, равная g на всех наборах множества A.*

Доказательство. Пусть $\widetilde{\alpha}_i = \left(\alpha_1^i, \ldots, \alpha_m^i\right)$, $g(\widetilde{\alpha}_i) = a_i$. Запишем систему линейных уравнений относительно $c_1, \ldots, c_{m+1}$:

$$c_1\alpha_1^i \oplus \cdots \oplus c_m\alpha_m^i \oplus c_{m+1} = a_1,$$

$$\ldots,$$

$$c_1\alpha_1^i \oplus \cdots \oplus c_m\alpha_m^i \oplus c_{m+1} = a_m.$$

Система совместна в силу существования функции $g(x_1, \ldots, x_m)$. Поскольку число неизвестных меньше числа уравнений, существует как минимум два решения данной системы. Одно определяет функцию g, другое — функцию $h(x_1, \ldots, x_m)$. Лемма 3 доказана.

Лемма 4. *Пусть* $g(x_1,\dots,x_m)=x_1\dots x_m$, $m\geqslant 2$, $A=\{\widetilde{\alpha}_1,\widetilde{\alpha}_2,\widetilde{\alpha}_3\}$ — *произвольное множество булевых наборов. Тогда существует линейная функция* $h(x_1,\dots,x_m)$, *которая равна* g *на* A.

Доказательство. Пусть на наборах множества A функция g равна a_1,a_2,a_3. Запишем систему линейных уравнений относительно коэффициентов $c_1,\dots,c_{m+1}$ линейной функции:

$$c_1\alpha_1^1\oplus\dots\oplus c_m\alpha_m^1\oplus c_{m+1}=a_1,$$
$$c_1\alpha_1^2\oplus\dots\oplus c_m\alpha_m^2\oplus c_{m+1}=a_2,$$
$$c_1\alpha_1^3\oplus\dots\oplus c_m\alpha_m^3\oplus c_{m+1}=a_3.$$

Достаточно показать, что ранг основной матрицы системы равен трём. Действительно, нулевых строк у данной матрицы нет, так как $(m+1)$-й элемент любой строки равен 1. Если сложить любые две строки этой матрицы, то нулевой строки не получится, так как все наборы множества A различны. Если сложить три строки, то в $(m+1)$-м элементе получившейся строки будет стоять 1. Поэтому строки основной матрицы линейно независимы, её ранг равен трём, система имеет хотя бы одно решение, которое задаёт некоторую линейную функцию $h(x_1,\dots,x_m)$, удовлетворяющую условию леммы. Лемма 4 доказана.

Пусть $\delta(\alpha_1,\dots,\alpha_m)=\sum\limits_{i=0}^{m-1}\alpha_i 2^i$ и

$$\mu_{r,s}(x_1,\dots,x_r,y_1,\dots,y_s)=\bigvee_{\substack{\sigma_1,\dots,\sigma_r:\\ \delta(\sigma_1,\dots,\sigma_r)<s}} x_1^{\sigma_1}\dots x_r^{\sigma_r}y_{\delta(\sigma_1,\dots,\sigma_r)+1}.$$

Переменные $x_1,\dots,x_r$ назовём *адресными*, переменные $y_1,\dots,y_s$ — *информационными*. Функция $\mu_{r,s}$ будет использоваться при получении нижних оценок.

2. Основные результаты

Здесь и далее, говоря о слипаниях, будем подразумевать линейные локальные k-кратные слипания.

Теорема 1. *Для любой бесконечной возрастающей последовательности натуральных чисел* n *и любой бесконечно возрастающей последовательности нечётных натуральных чисел* k *такой, что* $k=o(n)$, *имеет место соотношение* $L^*(n,k)\sim n$. *Для любой бесконечной возрастающей последовательности натуральных чисел* n *и любой бесконечно возрастающей последовательности чётных натуральных чисел* k *такой, что* $k=o(n)$, *имеет место соотношение* $4\frac{n}{k}\lesssim L^*(n,k)\lesssim 12\frac{n}{k}$

Доказательство. Начнём с верхней оценки. Пусть у $f(x_1, \ldots, x_n)$ все переменные существенны. Будем строить множества наборов T_1^*, T_2^*, являющиеся проверяющими тестами при нечётном и чётном k соответственно.

Добавим в T_1^* и T_2^* проверяющее множество $S_k(f)$ для функции f.

Если произошло слипание переменных, не принадлежащих одному множеству линейности, то для каких-то двух из данных переменных в $S_k(f)$ есть проверяющая пара. Если в соответствующей функции слипания эти две переменные существенны, то неисправность обнаружена. Если хоть одна из этих переменных стала фиктивной, то в $S_k(f)$ есть правильное ребро данного направления, на одном из наборов которого неисправность обнаружится.

Пусть переменные $x_i, \ldots, x_{i+r}$, $r \geqslant k-1$, составляют линейно нерасширяемое множество. Зафиксируем значения остальных переменных. Тогда по лемме 2 будет реализовываться одна из четырёх линейных функций. Поскольку все переменные f существенны, найдутся $\beta_1, \ldots, \beta_{i-1}$, $\beta_{i+r+1}, \ldots, \beta_n$ такие, что $f(\beta_1, \ldots, \beta_{i-1}, x_i, \ldots, x_{i+r}, \beta_{i+r+1}, \ldots, \beta_n) = x_i \oplus \cdots \oplus x_{i+r} \oplus d$, где $d = d(\beta_1, \ldots, \beta_{i-1}, \beta_{i+r+1}, \ldots, \beta_n) \in \{0, 1\}$. Если k чётное, то при слипании любых подряд идущих переменных из $x_i, \ldots, x_{i+r}$ слившиеся переменные станут фиктивными, так как вместо каждой из них подставляется одна и та же величина. В таком случае достаточно добавить в тест правильные рёбра для переменных $x_{i-1+k}, x_{i-1+2k}, \ldots, x_{i-1+\lfloor \frac{r+1}{k} \rfloor k}$, и неисправность будет проверена. Если k нечётное, то добавим в тест n-мерный набор $(\beta_1, \ldots, \beta_{i-1}, 1, \ldots, 1, \beta_{i+r+1}, \ldots, \beta_n)$ и все соседние ему наборы по переменным $x_i, \ldots, x_{i+r}$. Это обнаружит слипания любых k подряд идущих переменных из $x_i, \ldots, x_{i+r}$, если у соответствующей функции слипания есть фиктивные переменные (добавлены правильные рёбра направлений $x_i, \ldots, x_{i+r}$). Если функция слипания есть сумма всех переменных, то такое слипание не меняет функции, необходимость в проверке отсутствует. Если функция слипания есть отрицание суммы всех переменных, это могло быть не обнаружено из-за наличия слипаний других переменных. Такой случай будет рассмотрен далее.

Для случая, когда k чётное, проверяющий тест построен. На каждые k переменных линейно нерасширяемого множества приходится два набора (результат можно улучшить, но это не будет влиять на оценку). Тогда всего в T_2^* было добавлено асимптотически не более чем $12\frac{n}{k}$ наборов.

В случае нечётного k непроверенным остаётся только случай, когда произошло несколько слипаний, причём если слипаются перемен-

ные $x_i, \ldots, x_{i+k-1}$, то они принадлежат одному множеству линейности и функция слипания равна $x_i \oplus \cdots \oplus x_{i+k-1} \oplus 1$. Пусть $X_1, \ldots, X_u$ — множества линейности функции $f(x_1, \ldots, x_n)$. Заметим, что они необязательно состоят из подряд идущих переменных. Представим функцию $f(x_1, \ldots, x_n)$ как суперпозицию некоторой функции $g(y_1, \ldots, y_u)$ и линейных функций вида $l(z_1, \ldots, z_v) = z_1 \oplus z_2 \oplus \cdots \oplus z_v$.

Чтобы получить значение функции $g(y_1, \ldots, y_u)$ на произвольном наборе $(\alpha_1, \ldots, \alpha_u)$, нужно выбрать значения $\beta_1, \ldots, \beta_n$ переменных $x_1, \ldots, x_n$ такие, что сумма по модулю 2 значений переменных из i-го множества линейности X_i равна α_i, тогда $f(\beta_1, \ldots, \beta_n)$ и будет значением $g(y_1, \ldots, y_u)$ на наборе $(\alpha_1, \ldots, \alpha_u)$. Функция $g(y_1, \ldots, y_u)$ не зависит от того, какие именно значения выбирались для переменных произвольного множества линейности из $x_1, \ldots, x_n$, важна только их сумма по модулю 2.

Приведём пример. Пусть $f(x_1, x_2, \ldots, x_7) = (x_1 \oplus x_2 \oplus x_3)(x_4 \oplus x_5 \oplus x_6)x_7 \vee (x_1 \oplus x_2 \oplus x_3 \oplus 1)(x_4 \oplus x_5 \oplus x_6 \oplus 1)\overline{x}_7$. Тогда получаем суперпозицию $g(y_1, y_2, y_3) = y_1 y_2 y_3 \vee (y_1 \oplus 1)(y_2 \oplus 1)\overline{y}_3$ функций $y_1(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$, $y_2(x_4, x_5, x_6) = x_4 \oplus x_5 \oplus x_6$ и $y_3(x_7) = x_7$.

Если среди переменных множества линейности функции f произошло одно или несколько слипаний указанного типа, то это либо не меняет исходной функции, либо эквивалентно инверсии соответствующей переменной функции g. Для $g(y_1, \ldots, y_u)$ можно построить полный проверяющий тест относительно инверсий переменных мощностью не более чем u [4]. По данному тесту легко построить оставшиеся u наборов для T_1^*.

Оценим число наборов в T_1^*. Число линейно нерасширяемых множеств мощностью не менее чем k не превосходит $\frac{n}{k}$. Если суммарное число переменных в них равно s, то число добавленных в тест наборов не превосходит $\left(10\frac{n}{k}\right) + \left(s + \frac{n}{k}\right) + r$. Первое слагаемое соответствует $S_k(f)$, второе — правильным рёбрам для переменных линейно нерасширяемых множеств, третье — тесту на инверсии. Поскольку любое линейно нерасширямое множество целиком лежит в некотором множестве линейности, легко видеть, что $us \leqslant n - s + \frac{n}{k}$. Получаем итоговую оценку $|T_1^*| \leqslant n + 12\frac{n}{k}$.

Перейдём к нижней оценке. Оценим снизу $L^*(n, k)$ при нечётном k. Пусть $r = \left\lceil \log_2 \frac{n}{k} \right\rceil$, $s = \left\lfloor \frac{n-r}{k} \right\rfloor$. Рассмотрим функцию $f(x_1, \ldots, x_n) = x_{r+sk+1} \ldots x_n \mu_{r,s}(x_1, \ldots, x_r, x_{r+1} \oplus x_{r+2} \oplus \cdots \oplus x_{r+k}, x_{r+k+1} \oplus \cdots \oplus x_{r+2k}, \ldots, x_{r+(s-1)k+1} \oplus \cdots \oplus x_{r+sk})$. Будем далее считать переменные $x_{r+s+1}, \ldots, x_n$ равными единице. В общем случае обнаружить слипание переменных $x_{r+1}, \ldots, x_{r+k}$ можно только при наборе значений адресных перемен-

ных $(0,0,\ldots,0)$. Зафиксировав таким образом $x_1,\ldots,x_r$, получаем, что в исправном состоянии должна реализовываться функция $x_{r+1}\oplus x_{r+2}\oplus\cdots\oplus x_{r+k}$, а в случае слипания $x_{r+1},x_{r+2},\ldots,x_{r+k}$ может реализовываться любая линейная функция. Чтобы отличить верную линейную функцию от остальных возможных, по лемме 3 необходимо не менее чем $k+1$ наборов. Обнаружить слипание переменных $x_{r+jk+1},\ldots,x_{r+(j+1)k}$, $0\leqslant j\leqslant s-1$, можно только при значениях адресных переменных $\left(\sigma_1^j,\ldots,\sigma_k^j\right)$ таких, что $\delta\left(\sigma_1^j,\ldots,\sigma_2^j\right)=j$. Как и на первом шаге, для этого потребуется $k+1$ наборов. Поэтому для каждого j в тесте должно быть $k+1$ наборов. Для всех j должно быть $s(k+1)$ наборов. Поскольку при разных j наборы значений адресных переменных $\left(\sigma_1^j,\ldots,\sigma_k^j\right)$ не равны между собой, среди описанных наборов теста не может быть двух одинаковых наборов. В итоге получаем, что при указанных условиях на k и n число наборов проверяющего теста асимптотически не меньше n.

Теперь оценим снизу $L^*(n,k)$ при чётном k. Доказательство проводится аналогично случаю с нечётным k, только в качестве информационных переменных подаётся s конъюнкций: $x_{r+1}\&x_{r+2}\&\ldots\&x_{r+k}$, $\ldots$, $x_{r+(s-1)k+1}\&\ldots\&x_{r+sk}$. Используется лемма 4 о том, что отличить конъюнкцию от линейных функций можно, используя не менее 4 наборов (для построения подобных наборов достаточно установить в единицы все переменные, кроме двух, а этим двум придать всевозможные значения). При указанных условиях на k, n число информационных переменных асимптотически равно $\frac{n}{k}$, для каждой необходимо 4 набора. Теорема 1 доказана.

Теорема 2. *При $n\to\infty$, $k\to\infty$, $k=o(n)$, справедливо соотношение $L(n,k)\sim 2n$.*

Доказательство. Докажем сначала верхнюю оценку. Возьмём произвольную функцию $f(x_1,\ldots,x_n)$ и будем строить для неё проверяющий тест T. Первым действием добавим в T проверяющее множество $S_k(f)$.

Пусть переменные $x_i,\ldots,x_{i+r}$, $r\geqslant k-1$, составляют линейно-фиктивно нерасширяемое множество. Если все данные переменные фиктивны, то их слипания не меняют функции, поэтому в тест не добавляется ничего, переходим к следующему линейно-фиктивно нерасширяемому множеству. Пусть $x_{i_1},\ldots,x_{i_p}$ — все существенные переменные в данном множестве. Из леммы 2 следует, что существуют числа $\beta_1,\ldots,\beta_{i-1},\beta_{i+r+1},\ldots,\beta_n$ такие, что $f(\beta_1,\ldots,\beta_{i-1},x_i,\ldots,x_{i+r},\beta_{i+r+1},\ldots,\beta_n)=x_{i_1}\oplus\cdots\oplus x_{i_p}\oplus d$, где $d=d(\beta_1,\ldots,\beta_{i-1},\beta_{i+r+1},\ldots,\beta_n)\in\{0,1\}$. Это также линейная функция. Добавим в T n-мерный набор $(\beta_1,\ldots,\beta_{i-1},1,\ldots,1,\beta_{i+r+1},\ldots,\beta_n)$ и все соседние ему наборы по переменным $x_i,\ldots,x_{i+r}$. Если множество

существенных переменных изменилось в результате слипания, то на одном из добавленных наборов это обнаружится. Остаётся только неисправность, при которой вместо функции $x_{i_1} \oplus \cdots \oplus x_{i_p} \oplus d$ реализуется её отрицание. В зависимости от слипаний остальных переменных это либо приведёт к инверсии некоторого множества линейности, либо не изменит функции. Подобная неисправность будет обнаружена на последнем шаге (см. доказательство теоремы 1).

Основное отличие данного доказательства от доказательства теоремы 1 в том, что следующее рассматриваемое линейно-фиктивно нерасширяемое множество может начинаться с x_{i_p+1}, а не с x_{i+r+1} (оно не может начинаться с переменной ещё меньшего индекса, потому что переменные x_{i_p} и x_{i+r+1} существенны и находятся в разных множествах линейности). Это значит, что фиктивная переменная x_j может принадлежать двум линейно-фиктивно нерасширяемым множествам: множеству, в котором находится существенная переменная с наибольшим индексом, предшествующим j, и множеству, в котором находится существенная переменная с наименьшим индексом, превосходящим j. Поэтому число линейно-фиктивно нерасширяемых множеств мощностью не менее чем k можно оценить сверху через $2\frac{n}{k}$.

Необнаруженными остались только неисправности, связанные с инверсиями множеств линейности. Их проверяем тестом на инверсии описанным в теореме 1 способом. Единственное отличие состоит в том, что только существенные переменные линейно-фиктивно нерасширяемого множества принадлежат одному множеству линейности. Но фиктивные переменные образуют отдельное множество линейности, которое будет соответствовать фиктивной переменной функции g и которую можно отбросить.

Теперь подсчитаем число добавленных в T наборов. Пусть суммарное число переменных в линейно-фиктивно нерасширяемых множествах мощностью не менее k равно s, а число самих подмножеств равно t. Тогда число наборов можно оценить сверху так:

$$|S_k(f)| + (2s - t + t) + (n - s + t) \leqslant 2n + 17\frac{n}{k}.$$

Смысл первого слагаемого ясен. Во втором слагаемом вычитается t, так как либо в линейно-фиктивно нерасширяемом множестве есть хотя бы одна существенная переменная, которая не принадлежит другим линейно-фиктивно нерасширяемым множествам, либо все переменные данного множества фиктивны и оценка тем более верна. Также во втором слагаемом далее прибавляется t, так как каждому линейно-фиктивному

множеству соответствует набор, на котором все переменные множества равны единице и который не учтён ранее. Третье слагаемое получается аналогично тому, как при доказательстве теоремы 1 с учётом наличия фиктивной переменной функции g. Отсюда следует верхняя оценка.

Пусть $r = \lceil \log_2 2\frac{n}{k+1} \rceil$ и $s = 2\lfloor \frac{n-r}{k+1} \rfloor$. Рассмотрим функцию

$$f(x_1, \ldots, x_n) \\ = \mu_{r,s}(x_1, \ldots, x_r, x_{r+1}, x_{r+k+1}, x_{r+k+2}, x_{r+2k+2}, x_{r+2k+3}, \ldots, x_{r+\frac{s}{2}(k+1)}).$$

Пусть $0 \leqslant j \leqslant \frac{s}{2} - 1$. Рассмотрим слипания переменных $x_{r+1+j(k+1)}, \ldots, x_{r-1+(j+1)(k+1)}$ функции $f(x_1, \ldots, x_n)$. Ясно что при их слипании значение функции может поменяться только при таком наборе $\left(\sigma_1^{2j}, \ldots, \sigma_r^{2j}\right)$ значений адресных переменных, что $\delta\left(\sigma_1^{2j}, \ldots, \sigma_r^{2j}\right) = 2j$. Зафиксировав таким образом $x_1, \ldots, x_r$, получаем, что в исправном состоянии должна реализовываться функция $x_{r+1+j(k+1)}$. В неисправном состоянии может реализовываться любая линейная функция переменных $x_{r+1+j(k+1)}, \ldots, x_{r-1+(j+1)(k+1)}$. По лемме 3 необходимо как минимум $k+1$ наборов, чтобы отличить линейную функцию x_{r+1} от остальных возможных. Обнаружить слипание переменных $x_{r+2+j(k+1)}, \ldots, x_{r+(j+1)(k+1)}$ можно только при наборе $\left(\sigma_1^{2j+1}, \ldots, \sigma_r^{2j+1}\right)$ значений адресных переменных таком, что $\delta\left(\sigma_1^{2j+1}, \ldots, \sigma_r^{2j+1}\right) = 2j+1$, и на это также потребуется $k+1$ наборов. Таким образом, чтобы обнаружить слипание каждой из переменных $x_{r+1}, x_{r+k+1}, x_{r+k+2}, \ldots, x_{r+\frac{s}{2}(k+1)}$ с соседними ей $k-1$ фиктивными переменными, необходимо суммарно $s(k+1)$ наборов, причём среди данных наборов нет совпадающих. При $n \to \infty$, $k \to \infty$, $k = o(n)$, получаем, что число наборов проверяющего теста подобной функции асимптотически не меньше $2n$. Теорема 2 доказана.

ЛИТЕРАТУРА

1. **Романов Д. С.** О полных проверяющих тестах относительно локальных слипаний переменных в булевых функциях // Уч. зап. Казан. гос. ун-та. Сер. Физ.-мат. науки. 2009. Т. 151, №2. С. 197–206.
2. **Морозов Е. В.** О тестах относительно множественных линейных слипаний переменных в булевых функциях // Вестн. Москов. ун-та. Сер. 15. Вычисл. математика и кибернетика. 2014. №1. С. 22–25.
3. **Морозов Е. В., Романов Д. С.** О тестах относительно локальных линейных слипаний переменных в булевых функциях // Вестн. Нижегород. ун-та им. Н. И. Лобачевского. Сер. Физ.-мат. науки. 2012. №5. С. 153–158.
4. **Погосян Г. Р.** О проверяющих тестах для входов логических устройств. М: ВЦ АН СССР, 1982. 57 с.

5. Романов Д. С. О диагностических тестах относительно локальных слипаний переменных в булевых функциях // Прикл. математика и информатика. 2010. Т. 36. С. 91—98.

Евгений Валерьевич Морозов,
Дмитрий Сергеевич Романов

Статья поступила
11 июля 2014 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
January–February 2015. Volume 22, No. 1. P. 51–63

UDC 519.718

FULL DETECTING TESTS FOR BOOLEAN FUNCTIONS FOR LOCAL LINEAR FAULTS OF CIRCUITS' INPUTS

E. V. Morozov[1], *D. S. Romanov*[1]
[1]Lomonosov Moscow State University,
1 Leninskie gory, 119992 Moscow, Russia
e-mail: morozov_msu@mail.ru, romanov@cs.msu.ru

Abstract. Let a linear conglutination of variables in Boolean functions be a substitution of a linear function depending on these variables for them. The conglutination is local if all conglutinated variables are situated next to each other. Complete and single detecting tests are studied. Bibliogr. 5.

Keywords: test, Boolean function, conglutination.

REFERENCES

1. **D. S. Romanov**, On full detecting tests for local conglutinations of variables in Boolean functions, *Uch. Zap. Kazan. Gos. Univ., Ser. Fiz.-Mat. Nauki,* **151**, No. 2, 197–206, 2009.
2. **E. V. Morozov**, Tests for multiple linear conglutinations of variables in Boolean functions, *Vestn. Mosk. Univ., Ser.* 15, No. 1, 22a–26, 2014. Translated in *Mosc. Univ. Comput. Math. Cybern.,* **38**, No. 1, 21–25, 2014.
3. **E. V. Morozov** and **D. S. Romanov**, On tests for local linear conglutinations of variables in Boolean functions, *Vestn. Nizhegorod. Univ., Ser. Fiz.-Mat. Nauki,* No. 5, 153–158, 2012.
4. **G. R. Pogosyan**, *O proveryayushchikh testakh dlya vkhodov logicheskikh ustroistv* (On Detecting Tests for Logical Circuit Inputs), VTs AN SSSR, Moscow, 1982.

5. D. S. Romanov, Diagnostic tests for local coalescences of variables in Boolean functions, *Prikl. Mat. Inform.,* No. 36, 91–98, 2010. Translated in *Comput. Math. Model.,* **23**, No. 1, 72–78, 2012.

Evgeniy V. Morozov,
Dmitriy S. Romanov

Received
11 July 2014