

УДК 519.718

О ПОЛНЫХ ПРОВЕРЯЮЩИХ ТЕСТАХ ОТНОСИТЕЛЬНО ЛОКАЛЬНЫХ СЛИПАНИЙ ПЕРЕМЕННЫХ В БУЛЕВЫХ ФУНКЦИЯХ

И.А. Кузнецов, Д.С. Романов

Аннотация

Под локальным k -кратным слипанием переменных в булевой функции $f(\tilde{x}^n)$ понимается функция, полученная в результате подстановки вместо каждой из каких-то k последовательных переменных функции f произвольной булевой функции от этих переменных ($2 \leq k \leq n$). В работе изучаются полные проверяющие тесты относительно локальных k -кратных слипаний переменных в булевых функциях $f(\tilde{x}^n)$. При этом устанавливается, что при $n \rightarrow \infty$, $(n - k) \rightarrow \infty$, $k \rightarrow \infty$ асимптотика функции Шеннона длины такого теста имеет вид $2^{k-1}(n - k + 2)$. Кроме того, доказывается, что при $n \rightarrow \infty$, $(n - k) \rightarrow \infty$, $\gamma(n, k) \rightarrow \infty$, $\gamma(n, k) = o(\log_2(n - k))$ существует множество наборов мощности, не превосходящей $\lceil \log_{4/3}(n - k + 1) + \gamma(n, k) \rceil$, являющееся полным проверяющим тестом относительно локальных k -кратных слипаний переменных для почти всех булевых функций $f(\tilde{x}^n)$. В работе также получено, что при $n \rightarrow \infty$, $2 \leq k \leq n$, $(n - k) \rightarrow \infty$ для почти всех булевых функций $f(\tilde{x}^n)$ длина минимального полного проверяющего теста относительно локальных k -кратных слипаний переменных не превосходит 3.

Ключевые слова: булева функция, тест для входов схем, локальное слипание переменных.

Введение

Пусть n, k – натуральные числа ($1 \leq k \leq n$), $f(\tilde{x}^n)$ – булева функция и $\Phi(\tilde{y}^k) = \{\varphi_i(\tilde{y}^k) \mid i = 1, \dots, 2^{2^k}\}$ – система всевозможных попарно неравных булевых функций k переменных. Обозначим через $\Psi = \Psi_{n,k,f,\Phi}(\tilde{x}^n)$ систему функций, в которую входит функция $f(\tilde{x}^n)$ и всевозможные функции $\psi_{j,i}(\tilde{x}^n)$ вида $\psi_{j,i}(\tilde{x}^n) = f(x_1, \dots, x_{j-1}, \underbrace{\varphi_i(x_j, x_{j+1}, \dots, x_{j+k-1})}_{k \text{ раз}}, \dots, \varphi_i(x_j, x_{j+1}, \dots, x_{j+k-1}), x_{j+k}, \dots, x_n)$,

где $1 \leq j \leq n - k + 1$, $i \in \{1, \dots, 2^{2^k}\}$. Ясно, что $|\Psi| = 2^{2^k}(n - k + 1) + 1$. Множество T наборов значений переменных x_1, \dots, x_n называется *полным проверяющим тестом относительно локальных k -кратных слипаний переменных булевой функции $f(\tilde{x}^n)$* тогда и только тогда, когда любая не равная $f(\tilde{x}^n)$ функция из Ψ отличается от f на множестве T . Число наборов в тесте T называется его *длиной* и обозначается $l(T)$. Тест минимальной длины называется *минимальным*. Длину минимального полного проверяющего теста относительно локальных k -кратных слипаний переменных булевой функции $f(\tilde{x}^n)$ будем обозначать через $L_k(f(\tilde{x}^n))$. Введем *функцию Шеннона длины полного проверяющего теста относительно локальных k -кратных слипаний переменных булевой функции*: $L_k(n) = \max_{f(\tilde{x}^n)} L_k(f(\tilde{x}^n))$.

Ранее рядом авторов изучались некоторые близкие к рассматриваемым в данной работе тесты при неисправностях переменных в булевых функциях n переменных (так называемые тесты для входов схем). Следует отметить цикл работ

В.Н. Носкова [1–4], статью Н.Н. Нурмеева [5] и препринт Г.Р. Погосяна [6]. Были установлены точные значения функций Шеннона длин тестов следующих типов: полного проверяющего теста при константных неисправностях на входах схем [2] и единичного диагностического теста при константных неисправностях на входах схем [3], полного проверяющего теста при дизъюнктивных слипаниях переменных и проверяющего теста при дизъюнктивных слипаниях переменных кратности не более k [6], единичного проверяющего теста при инверсиях на входах схем [6]. С точностью до аддитивной константы 1 найдена функция Шеннона длины полного проверяющего теста при инверсиях на входах схем [6]. В [1] установлены асимптотика логарифма функции Шеннона длины диагностического теста относительно константных неисправностей кратности не более k на входах схем (при $n \rightarrow \infty$, $k = o(n)$) и порядок логарифма функции Шеннона длины полного диагностического теста относительно константных неисправностей. В [3] доказана логарифмичность по n длины минимального единичного диагностического теста относительно константных неисправностей на входах для почти всех булевых функций n переменных. В [2] для почти всех булевых функций при константных неисправностях на входах схем доказаны линейность длины минимального полного проверяющего теста и равенство трем длины минимального единичного проверяющего теста. В [4, 5] рассмотрены классы произвольных неисправностей, преобразующих информацию на не более чем k входах, и было доказано, что для почти всех булевых функций n переменных при постоянном k существует стандартный диагностический тест логарифмической по n длины [4] и что при случайном выборе множества наборов некоторой логарифмической по n мощности при постоянном k это множество почти всегда образует диагностический тест [5].

1. Поведение функции Шеннона $L_k(n)$

Верно следующее утверждение о поведении функции Шеннона $L_k(n)$.

Теорема 1. Пусть $n, k \in N$, $2 \leq k \leq n$. Тогда справедливы неравенства:

$$2^{k-1}(n - k + 2) \leq L_k(n) \leq (2^{k-1} + 1) \cdot (n - k + 1) + 2^k \left\lceil \frac{n - k + 1}{k} \right\rceil.$$

Доказательство. Таблицу размерами $2^k \times 2^{2^k}$, состоящую из столбцов значений всех функций из $\Phi(\tilde{y}^k)$, обозначим через $M(\Phi(\tilde{y}^k))$, а отрицание (поэлементное) этой таблицы – через $M(\bar{\Phi}(\tilde{y}^k))$. Зафиксируем число j ($1 \leq j \leq n - k + 1$). Рассмотрим таблицу неисправностей, построенную для произвольной булевой функции $f(\tilde{x}^n)$ на всех (следующих в лексикографическом порядке) наборах подкуба $B_{(k,j)}^{\tilde{\alpha}, \tilde{\beta}} = (\tilde{\alpha}^{j-1}, \tilde{2}^k, \tilde{\beta}^{n-j-k+1})$, где двойка обозначает произвольное значение переменной, а $\tilde{\alpha}^{j-1}$ и $\tilde{\beta}^{n-j-k+1}$ – булевы векторы. Вектор значений функции $f(\tilde{x}^n)$ на подкубе $B_{(k,j)}^{\tilde{\alpha}, \tilde{\beta}}$ обозначим через $f'[B_{(k,j)}^{\tilde{\alpha}, \tilde{\beta}}]$. Заметим, что если $f(\tilde{\alpha}^{j-1}, \tilde{0}^k, \tilde{\beta}^{n-j-k+1}) = f(\tilde{\alpha}^{j-1}, \tilde{1}^k, \tilde{\beta}^{n-j-k+1}) = \sigma$, то для любой функции $\psi_{j,i}(\tilde{x}^n)$ вектор $\psi_{j,i}[B_{(k,j)}^{\tilde{\alpha}, \tilde{\beta}}]$ равен $(\tilde{\sigma}^{2^k}) = (\sigma, \dots, \sigma)$. При этом если существует такой булев набор $\tilde{\delta}^k$, что $f(\tilde{\alpha}^{j-1}, \tilde{\delta}^k, \tilde{\beta}^{n-j-k+1}) \neq \sigma$, то этот набор проверяет все функции неисправностей $\psi_{j,1}(\tilde{x}^n), \dots, \psi_{j,2^k}(\tilde{x}^n)$. В этом случае тройку наборов $(\tilde{\alpha}^{j-1}, \tilde{0}^k, \tilde{\beta}^{n-j-k+1}), (\tilde{\alpha}^{j-1}, \tilde{1}^k, \tilde{\beta}^{n-j-k+1}), (\tilde{\alpha}^{j-1}, \tilde{\delta}^k, \tilde{\beta}^{n-j-k+1})$ такую, что $f(\tilde{\alpha}^{j-1}, \tilde{0}^k, \tilde{\beta}^{n-j-k+1}) = f(\tilde{\alpha}^{j-1}, \tilde{1}^k, \tilde{\beta}^{n-j-k+1}) \neq f(\tilde{\alpha}^{j-1}, \tilde{\delta}^k, \tilde{\beta}^{n-j-k+1})$ назовем *замечательной тройкой для x_j* , а набор $(\tilde{\alpha}^{j-1}, \tilde{\delta}^k, \tilde{\beta}^{n-j-k+1})$ – *особым набором для x_j* . Если $f(\tilde{\alpha}^{j-1}, \tilde{0}^k, \tilde{\beta}^{n-j-k+1}) = 0$, $f(\tilde{\alpha}^{j-1}, \tilde{1}^k, \tilde{\beta}^{n-j-k+1}) = 1$, то фрагмент таблицы неисправностей, связанный с проверкой переменных x_j, \dots, x_{j+k-1} ,

на подкубе $B_{(k,j)}^{\tilde{\alpha},\tilde{\beta}}$ имеет вид $M(\Phi(\tilde{y}^k))$. Если же $f(\tilde{\alpha}^{j-1}, \tilde{0}^k, \tilde{\beta}^{n-j-k+1}) = 1$, $f(\tilde{\alpha}^{j-1}, \tilde{1}^k, \tilde{\beta}^{n-j-k+1}) = 0$, то фрагмент таблицы неисправностей, связанный с проверкой переменных x_j, \dots, x_{j+k-1} , на подкубе $B_{(k,j)}^{\tilde{\alpha},\tilde{\beta}}$ имеет вид $M(\bar{\Phi}(\tilde{y}^k))$. Ясно, что в последних двух случаях для проверки всех функций неисправностей $\psi_{j,1}(\tilde{x}^n), \dots, \psi_{j,2^{2^k}}(\tilde{x}^n)$ достаточно взять все наборы подкуба $B_{(k,j)}^{\tilde{\alpha},\tilde{\beta}}$ и еще один некоторый набор.

Доказательство верхней оценки. Пусть $f(\tilde{x}^n)$ – произвольная булева функция. Под *проверкой переменной* x_j будем понимать процесс построения множества наборов, обнаруживающих всевозможные слипания переменных x_j, \dots, x_{j+k-1} . Организуем процесс построения теста для $f(\tilde{x}^n)$ следующим образом. Будем последовательно строить множества наборов, проверяющих сначала переменную x_{n-k+1} , затем переменную x_{n-k} , затем x_{n-k-1} и т. д., наконец переменную x_1 . Проверку каждой переменной будем называть *шагом*.

Одной из типичных ситуаций будет использование для проверки переменной x_j всех 2^k наборов некоторого подкуба $B_{(k,j)}^{\tilde{\alpha},\tilde{\beta}}$ и еще одного набора. При этом под *наследованием* будет пониматься ситуация, когда для проверки x_{j-1} используется половина наборов выбранного на предыдущем шаге подкуба $B_{(k,j)}^{\tilde{\alpha},\tilde{\beta}}$ (входящая в некоторый подкуб $B_{(k,j-1)}^{\tilde{\alpha}',\tilde{\beta}'}$).

Договоримся о некоторых терминах, связанных с классификацией векторов $f[B_{(k,j)}^{\tilde{\alpha},\tilde{\beta}}] = (\xi_1, \dots, \xi_{2^k})$. Если все компоненты вектора одинаковы, назовем вектор *константным*. Если вектор порождает замечательную тройку по x_j , назовем его *замечательным*. Если в векторе найдутся две не равные друг другу компоненты, отстоящие одна от другой на расстоянии 2^{k-1} , то соответствующие этой паре компонент входные наборы функции f назовем *перспективной парой*. Если при этом в векторе первая и последняя компоненты не равны друг другу, то вектор назовем *перспективным*. Остальные векторы $f[B_{(k,j)}^{\tilde{\alpha},\tilde{\beta}}]$, в которых первая и последняя компоненты не равны друг другу, назовем *бесперспективными* (ясно, что первая половина бесперспективного вектора равна второй его половине).

Два подкуба $B_{(k,j)}^{\tilde{\alpha}',\tilde{\beta}'}$ и $B_{(k,j)}^{\tilde{\alpha}'',\tilde{\beta}''}$ (а также соответствующие им вектора $f[B_{(k,j)}^{\tilde{\alpha}',\tilde{\beta}'}]$ и $f[B_{(k,j)}^{\tilde{\alpha}'',\tilde{\beta}''}]$) назовем *соседними*, если наборы $\tilde{\alpha}'$ и $\tilde{\alpha}''$ отличаются лишь последними компонентами.

Опишем очередной шаг построения теста, связанный с проверкой x_j , рассматривая различные случаи.

1. Если для данной переменной существует замечательная тройка, то ее особый набор проверяет данную переменную; включим его в тест, перейдем к следующему шагу.

2. Если замечательных троек нет, но есть перспективная пара наборов, то рассмотрим k подкубов размерности k , содержащих эту пару наборов: $B_{(k,j)}^{\tilde{\alpha},\tilde{\beta}}$, $B_{(k,j-1)}^{\tilde{\alpha}^{(2)},\tilde{\beta}^{(2)}}$, \dots , $B_{(k,j-k+1)}^{\tilde{\alpha}^{(k)},\tilde{\beta}^{(k)}}$ (половина наборов каждого следующего подкуба содержится в предыдущем). Каждый из этих подкубов имеет неконстантный вектор. Можно завершить k шагов построения теста, включив в тест все наборы этих кубов и еще k наборов. При этом на каждом шаге будет, очевидно, иметь место наследование, и общее число включенных в тест наборов не превзойдет величины $2^{k-1}(k+1) + k$.

3. Если все подкубы $B_{(k,j)}^{\tilde{\alpha},\tilde{\beta}}$ имеют константные векторы значений, то любой набор не позволит обнаружить никакое слипание переменных x_j, \dots, x_{j+k-1} . В тест добавить нечего, шаг завершен.

4. Рассмотрим, наконец, ситуацию, когда среди векторов $f[B_{(k,j)}^{\tilde{\alpha}, \tilde{\beta}}]$ встречаются лишь константные и бесперспективные векторы, но не одни только константные.

4.1. Пусть среди всех векторов $f[B_{(k,j)}^{\tilde{\alpha}, \tilde{\beta}}]$ найдутся два соседних различных бесперспективных вектора либо соседние – бесперспективный и константный векторы. Тогда на данном шаге включим в тест все входные наборы для бесперспективного вектора и еще один набор, а на следующем шаге один из векторов значений, который «покрывается» данными двумя соседними, будет либо замечательным (тогда за 2 шага в тест будет включено $2^k + 2$ наборов), либо перспективным, причем в данном случае будет иметь место наследование, и по аналогии с п. 2 можно провести еще k шагов с наследованием; общее число включенных в тест на всех этих $(k + 1)$ шагах наборов составит не более чем $2^{k-1}(k + 2) + k + 1$.

4.2. Пусть теперь среди всех векторов $f[B_{(k,j)}^{\tilde{\alpha}, \tilde{\beta}}]$ есть два соседних различных константных вектора и встречаются одинаковые соседние бесперспективные векторы. Тогда на данном шаге включим в тест все входные наборы для некоторого бесперспективного вектора и еще один набор, а на следующем шаге любой из векторов, «покрываемых» двумя различными соседними константными векторами, будет перспективным, и по аналогии с п. 2 можно провести еще k шагов с наследованием; общее число включенных в тест на всех этих $(k + 1)$ шагах наборов составит не более чем $2^{k-1}(k + 3) + k + 1$.

4.3. Пусть среди всех векторов $f[B_{(k,j)}^{\tilde{\alpha}, \tilde{\beta}}]$ есть только либо соседние равные бесперспективные векторы (хотя бы одна пара), либо соседние равные константные векторы. В этом случае организуем наследование с использованием бесперспективных векторов соседних кубов. Заметим, что при «склейке» соседних одинаковых бесперспективных векторов на следующем шаге возникают либо константные, либо бесперспективные векторы.

4.3.1. Если все векторы $f[B_{(k,j)}^{\tilde{\alpha}, \tilde{\beta}}]$ одинаковы и бесперспективны, то через некоторое число m шагов с наследованием либо будет проверена переменная x_1 и в тест будет включено наборов не более чем $2^{k-1}(m + 1) + m$ (при этом построение теста завершится), либо появится непроверяемая переменная, и в тест будет включено наборов не более чем $2^{k-1}m + m$.

4.3.2. Если же не выполнено и условие предыдущего подпункта, то возможны следующие случаи:

А) можно организовать процесс включения наборов в тест так, что через некоторое число m шагов с наследованием бесперспективных векторов появится замечательный вектор, и за эти m шагов в тест войдет не более чем $2^{k-1}m + m$ наборов;

Б) можно организовать процесс включения наборов в тест так, что через некоторое число m шагов наследования бесперспективных векторов появится перспективный вектор, тогда можно проделать еще k шагов, как в п. 2, и за $m + k$ шагов в тест войдет не более чем $2^{k-1}(k + m + 1) + k + m$ наборов;

В) ситуации случаев А и Б не встречаются, и всякое наследование с использованием бесперспективных векторов приводит рано или поздно к константным векторам. Пусть m – максимальное число шагов в таком наследовании, и проверяется переменная x_{j-m+1} . Если у всех подкубов константные векторы, то эта переменная не проверяема, и в тест за m шагов войдет не более чем $2^{k-1}m + m - 1$ наборов. Иначе на некотором шаге t ($t \leq m$) найдутся два соседних подкуба с неравными векторами (сами эти векторы могут быть константными, тогда для проверки соответствующей переменной придется использовать «посторонний» подкуб), что приведет на шаге $t + 1$ к появлению перспективной пары наборов, далее по аналогии

с п. 2 можно проделать еще k шагов, и за $k + t + 1$ шагов в тест войдет не более чем $2^{k-1}(k + t + 3) + k + t + 1$ наборов.

Подытоживая все случаи, замечаем, что за каждые k шагов число наборов в тесте возрастает не более чем на $2^{k-1}(k + 2) + k$, откуда и получается верхняя оценка.

Доказательство нижней оценки. Рассмотрим в качестве булевой функции $f(\tilde{x}^n)$ конъюнкцию n переменных. Ясно, что в проверяющий тест должен войти набор $(\tilde{1}^n)$, а также все наборы, в которых наиболее удаленные друг от друга нули отстоят не более чем на $(k-1)$ место. Если не включить набор $(\tilde{1}^{j-1}, \tilde{\eta}^k, \tilde{1}^{n-j-k+1})$, то нельзя отличить от f такую функцию $\psi_{j,i}(\tilde{x}^n)$, для которой $\varphi_i(x_j, \dots, x_{j+k-1})$ обращается в 1 только на наборах $\tilde{\eta}^k$ и $(\tilde{1}^k)$. Ясно также, что выбранных наборов достаточно для проверки $f(\tilde{x}^n)$. Общее количество выбранных наборов, очевидно, равно $1 + n + \sum_{t=0}^{k-2} (n-i-1)2^i = 2^{k-1}(n-k+2)$, откуда и получается нижняя оценка функции Шеннона. \square

Следствие 1. Пусть $n, k \in N$, $2 \leq k < n$, $n \rightarrow \infty$, $(n-k) \rightarrow \infty$, $k \rightarrow \infty$. Тогда $L_k(n) \sim 2^{k-1}(n-k+2)$.

2. Тесты для почти всех булевых функций

Теорема 2. Пусть $n, k \in N$, $2 \leq k < n$, $n \rightarrow \infty$, $(n-k) \rightarrow \infty$, $\gamma(n, k) \rightarrow \infty$, $\gamma(n, k) = o(\log_2(n-k))$. Тогда существует множество наборов \mathcal{T}_n мощности $|\mathcal{T}_n| \leq \left\lceil \log_{4/3}(n-k+1) + \gamma(n, k) \right\rceil$, являющееся полным проверяющим тестом относительно локальных k -кратных слияний переменных для почти всех булевых функций $f(\tilde{x}^n)$.

Доказательство. Положим $q = \left\lceil \log_{4/3}(n-k+1) + \gamma(n, k) \right\rceil$ и выберем множество \mathcal{T}_n , состоящее из q булевых n -разрядных наборов таких, что в каждом из них нет k подряд идущих одинаковых значений, и, кроме того, таких, что для каждого j ($1 \leq j \leq n-k+1$) при всевозможных k -кратных локальных константных слияниях переменных с j -й по $(j+k-1)$ -ю из них получается множество $\hat{T}_{n,j}$, состоящее из $2q$ попарно неравных наборов. Такой выбор множества \mathcal{T}_n , очевидно, возможен. Оценим сверху число $\Omega_{n, \mathcal{T}_n}$ булевых функций n переменных, для которых множество \mathcal{T}_n не образует проверяющего теста рассматриваемого типа: $\Omega_{n, \mathcal{T}_n} \leq (n-k+1)6^q 2^{2^n - 3q}$. Здесь множитель $(n-k+1)$ означает число способов выбора переменной x_j , по которой в множествах \mathcal{T}_n и $\hat{T}_{n,j}$ нет замечательных троек, множитель 6^q есть число способов выбора значений функции f на наборах из \mathcal{T}_n и $\hat{T}_{n,j}$ так, что не возникает замечательных троек по x_j , множитель $2^{2^n - 3q}$ — это число способов доопределения значений функции f на остальных наборах. Имеем: $\Omega_{n, \mathcal{T}_n} \leq (n-k+1) (3/4)^q 2^{2^n} \leq (3/4)^{\gamma(n, k)} 2^{2^n} = o(2^{2^n})$, что и требовалось доказать. \square

Докажем далее, что при достаточно слабых ограничениях на k при растущих n значение функции $L_k(f(\tilde{x}^n))$ ограничено сверху величиной 3 для почти всех булевых функций $f(\tilde{x}^n)$.

$$\text{Положим } r = \left\lceil \frac{n-k+1}{3} \right\rceil, l = \left\lfloor \frac{r+k-2}{k} \right\rfloor.$$

Обозначим через U_n множество всех таких наборов $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ из E_2^n , у которых $\alpha_1 = \bar{\alpha}_2 = \alpha_{k+1} = \bar{\alpha}_{k+2} = \dots = \alpha_{lk+1} = \bar{\alpha}_{lk+2} = \dots = \alpha_{(l-1)k+1} = \bar{\alpha}_{(l-1)k+2} = \alpha_{lk+1}$ и, если $r > lk-k+2$ (то есть $r+k-1 > lk+1$), то $\alpha_1 = \bar{\alpha}_{lk+2}$.

Легко видеть, что каждый набор из U_n не содержит k одинаковых подряд идущих значений среди значений переменных x_1, \dots, x_{r+k-1} , и что

$$|U_n| = \begin{cases} 2^{n-2l-1}, & \text{если } r > lk - k + 2, \\ 2^{n-2l}, & \text{если } r = lk - k + 2. \end{cases} \quad (1)$$

Пусть $\tilde{\alpha} \in U_n$. Обозначим через $S_{n,k}^{\tilde{\alpha}}$ множество всех таких наборов $\tilde{\beta}$, каждый из которых получается из $\tilde{\alpha}$ заменой каких-то k подряд идущих значений (в позициях с 1 по $r+k-1$) одинаковыми цифрами (нулями или единицами). Положим $\widehat{S}_{n,k}^{\tilde{\alpha}} = S_{n,k}^{\tilde{\alpha}} \cup \tilde{\alpha}$. Заметим, что

$$r + 2 \leq |\widehat{S}_{n,k}^{\tilde{\alpha}}| \leq 2r + 1. \quad (2)$$

Положим $V_n = \bigcup_{\tilde{\alpha} \in U_n} S_{n,k}^{\tilde{\alpha}}$.

Обозначим через M_n множество наборов из U_n такое, что для любых различных $\tilde{\alpha}', \tilde{\alpha}''$ из M_n выполнено соотношение

$$S_{n,k}^{\tilde{\alpha}'} \cap S_{n,k}^{\tilde{\alpha}''} = \emptyset. \quad (3)$$

Введем функцию $\mu_k(n)$ – максимальную мощность такого множества M_n .

Лемма 1. *Справедливы оценки*

$$2^{n-2l-k-\log_2 r-1} \leq \mu_k(n) \leq 2^{n-2l-k+3},$$

где

$$l = \left\lfloor \frac{r+k-2}{k} \right\rfloor, \quad r = \left\lceil \frac{n-k+1}{3} \right\rceil.$$

Доказательство. *Верхняя оценка* следует из условия (3) в определении $\mu_k(n)$ и из неравенств (2):

$$\mu_k(n) \leq \frac{|V_n|}{\min_{\tilde{\alpha} \in U_n} |S_{n,k}^{\tilde{\alpha}}|} \leq \frac{2r}{r+1} \cdot 2^{n-2l-(k-2)} \leq 2^{n-2l-k+3}.$$

Нижняя оценка. Будем строить множество M_n такое, что $|M_n| = \mu_k(n)$, последовательно включая в него наборы. Заметим, что если набор $\tilde{\alpha}$ включен в M_n , то по определению M_n в это множество уже нельзя включить ни один из наборов $\tilde{\alpha}'''$, для которых $S_{n,k}^{\tilde{\alpha}} \cap S_{n,k}^{\tilde{\alpha}'''} \neq \emptyset$. Число таких $\tilde{\alpha}'''$ для фиксированного $\tilde{\alpha}$ не превосходит величины $r2^k$ (включая $\tilde{\alpha}$). Следовательно, выбрав t наборов в множество M_n , «запрещенными» становятся не более чем $tr2^k$ наборов. И если $tr2^k < |U_n|$, то в U_n еще есть набор, который можно включить в M_n , что противоречит максимальной мощности M_n . Значит, $|U_n| \leq \mu_k(n)r2^k$, то есть с учетом (1) $\mu_k(n) \geq 2^{n-2l-k-\log_2 r-1}$, что и доказывает лемму. \square

Теорема 3. *Пусть $n, k \in \mathbb{N}$, $n \rightarrow \infty$, $2 \leq k \leq n$, $(n-k) \rightarrow \infty$. Тогда для почти всех булевых функций $f(\tilde{x}^n)$ справедлива оценка $L_k(f(\tilde{x}^n)) \leq 3$.*

Доказательство. Покажем, что для почти всех булевых функций $f(\tilde{x}^n)$ найдется набор $\tilde{\eta} \in E_2^n$, на котором для любого $j \in \{1, \dots, r\}$ обнаруживаются все локальные k -кратные слипания переменных $x_j, x_{j+1}, \dots, x_{j+k-1}$ (из этого с очевидностью будет следовать утверждение теоремы).

Заметим, что для искомого набора $\tilde{\eta}$ достаточно, чтобы он лежал в U_n и обладал следующим свойством:

Свойство А. Для любого $\tilde{\beta} \in S_{n,k}^{\tilde{\eta}}$ выполнено равенство $f(\tilde{\beta}) = \bar{f}(\tilde{\eta})$.

Случай 1. Пусть $3 \leq k \leq n$.

Зафиксируем некоторое множество M_n ($M_n \subseteq U_n$) такое, что $|M_n| = \mu_k(n)$, и оценим сверху долю $P_{n,k}$ тех булевых функций $f(x_1, \dots, x_n)$, для которых не существует набора $\tilde{\eta}$ из M_n , обладающего свойством А:

$$P_{n,k} = \left(\prod_{\tilde{\alpha} \in M_n} \left(2^{|\hat{S}_{n,k}^{\tilde{\alpha}}|} - 2 \right) \cdot 2^{2^n - \sum |\hat{S}_{n,k}^{\tilde{\alpha}}|} \right) / \left(2^{2^n} \right),$$

где суммирование производится по $\tilde{\alpha} \in M_n$. Далее, используя (2) и лемму 1, получим:

$$P_{n,k} = \prod_{\tilde{\alpha} \in M_n} \left(1 - \frac{2}{2^{|\hat{S}_{n,k}^{\tilde{\alpha}}|}} \right) \leq \left(1 - \frac{2}{2^{2r+1}} \right)^{\mu_k(n)} \leq \left(1 - \frac{1}{2^{2(n-k+2)/3}} \right)^{2^{n-2l-k-\log_2 r-1}},$$

а последнее выражение стремится к нулю при $n \rightarrow \infty$, $3 \leq k \leq n$, $(n-k) \rightarrow \infty$. Значит, при указанных условиях набор $\tilde{\eta}$ существует в выбранном множестве M_n для почти всех булевых функций n переменных, что и требовалось установить для доказательства теоремы в данном случае.

Случай 2). Пусть теперь $k = 2$, $n \geq 11$ (тогда $r = \left\lfloor \frac{n-1}{3} \right\rfloor \geq 4$).

Доказательство аналогично случаю 1. Достаточно лишь заметить, что для любого $\tilde{\alpha} \in U_n$ верно неравенство:

$$r + 2 \leq |\hat{S}_{n,k}^{\tilde{\alpha}}| \leq r + 3.$$

Выберем для каждого фиксированного набора $(\alpha_1, \alpha_{r+2}, \alpha_{r+3}, \dots, \alpha_n)$ из E_2^{n-r} по одному набору $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ из U_n в множество M_n , тогда, очевидно, все сформулированные ранее требования на M_n выполнены и на $|M_n| = 2^{n-r}$. При этом

$$P_{n,k} = \prod_{\tilde{\alpha} \in M_n} \left(1 - \frac{2}{2^{|\hat{S}_{n,k}^{\tilde{\alpha}}|}} \right) \leq \left(1 - \frac{2}{2^{r+3}} \right)^{2^{n-r}},$$

а последнее выражение стремится к нулю при $n \rightarrow \infty$. Значит, при указанных условиях набор $\tilde{\eta}$ существует в выбранном множестве M_n для почти всех булевых функций n переменных, что и требовалось доказать. \square

Работа выполнена при поддержке РФФИ (проекты № 09-01- 00817 и 07-01-00444).

Summary

I.A. Kuznetsov, D.S. Romanov. On Full Checking Tests under Local Glueings of Variables in Boolean Functions.

A local k -fold glueing of variables in Boolean function $f(\tilde{x}^n)$ is a function obtained as a result of substitution instead of some k successive variables an arbitrary Boolean function depending on these variables ($2 \leq k \leq n$). Full checking tests under local k -fold glueings

of variables in Boolean functions $f(\tilde{x}^n)$ are studied in this paper. It is established that if $n \rightarrow \infty$, $(n - k) \rightarrow \infty$, $k \rightarrow \infty$, then an asymptotics of Shannon function of the test length is $2^{k-1}(n - k + 2)$. Furthermore, let $n \rightarrow \infty$, $(n - k) \rightarrow \infty$, $\gamma(n, k) \rightarrow \infty$, $\gamma(n, k) = o(\log_2(n - k))$, therefore, a set of n -tuples exists which is full checking test under local k -fold glueings of variables in almost all Boolean functions $f(\tilde{x}^n)$ and whose power is not greater than $\lceil \log_{4/3}(n - k + 1) + \gamma(n, k) \rceil$. At last, under conditions $n \rightarrow \infty$, $2 \leq k \leq n$, $(n - k) \rightarrow \infty$, a length of minimal full checking test under local k -fold glueings of variables is not greater than 3 for almost all Boolean functions $f(\tilde{x}^n)$.

Key words: Boolean function, test for inputs of circuits, local glueing of variables.

Литература

1. *Носков В.Н.* Диагностические тесты для входов логических устройств // Дискретный анализ. – Новосибирск: ИМ СО АН СССР, 1974. – № 26. – С. 72–83.
2. *Носков В.Н.* О сложности тестов, контролирующих работу входов логических схем // Дискретный анализ. – Новосибирск: ИМ СО АН СССР, 1975. – № 27. – С. 23–51.
3. *Носков В.Н.* О длинах минимальных единичных диагностических тестов, контролирующих работу входов логических схем // Методы дискретного анализа в синтезе управляющих систем. – Новосибирск: ИМ СО АН СССР, 1978. – № 32. – С. 40–51.
4. *Носков В.Н.* Об универсальных тестах для диагностики одного класса неисправностей комбинационных схем // Методы дискретного анализа в решении экстремальных задач. – Новосибирск: ИМ СО АН СССР, 1979. – № 33. – С. 41–52.
5. *Нурмеев Н.Н.* Об универсальных диагностических тестах для одного класса неисправностей комбинационных схем // Вероятностные методы и кибернетика. – Казань: Изд-во Казан. ун-та, 1982. – Вып. 18. – С. 73–76.
6. *Погосян Г.Р.* О проверяющих тестах для логических схем. – М.: ВЦ АН СССР, 1982. – 57 с.

Поступила в редакцию
02.03.09

Кузнецов Иван Алексеевич – студент факультета вычислительной математики и кибернетики Московского государственного университета им. М. В. Ломоносова.

E-mail: mk@cs.msu.ru

Романов Дмитрий Сергеевич – кандидат физико-математических наук, доцент факультета вычислительной математики и кибернетики Московского государственного университета им. М. В. Ломоносова.

E-mail: romanov@cs.msu.ru