

Московский государственный университет имени М. В. Ломоносова

На правах рукописи

УДК 519.718

Морозов Евгений Валерьевич

**Об оценках функций Шеннона длин тестов при некоторых
неисправностях входов схем**

Специальность 01.01.09 — дискретная математика и математическая
кибернетика

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:

к. ф.-м. н., доцент

Романов Д. С.

Москва – 2015

Содержание

Введение	4
1 Тестирование булевых функций относительно линейных слипаний	
переменных	16
1.1 Основные определения и обозначения	16
1.2 Проверяющий тест относительно множественных линейных слипаний переменных	18
1.3 Диагностические тесты относительно линейных слипаний переменных	26
1.4 Локальные k -кратные слипания переменных	33
2 Тестирование булевых функций относительно монотонных симметрических слипаний переменных	45
2.1 Основные определения и обозначения	45
2.2 Проверяющий тест относительно множественных монотонных симметрических слипаний переменных	46
2.3 Диагностический тест относительно монотонных симметрических слипаний переменных	60
2.4 Диагностический тест относительно дизъюнктивных слипаний переменных	61
3 Тестирование булевых функций относительно вытеснения переменных	64

3.1 Основные определения и обозначения	64
3.2 Проверяющий тест	65
3.3 Диагностический тест	72
Заключение	75
Литература	77

Введение

Данная работа является исследованием в области теории надежности и контроля управляющих систем. В качестве управляющих систем рассматриваются схемы, реализующие булевы функции. Схемы могут переходить в неисправные состояния. Возникает задача обнаружения и диагностики неисправностей. Данная задача впервые была поставлена в работах И. А. Чегис и С. В. Яблонского [43, 44] Ими были предложены логические методы контроля управляющих систем. На входы схемы подаются специальным образом подобранные значения входных переменных $x_1, \dots, x_n$, от которых зависит реализуемая булева функция. По получившимся выходным значениям схемы можно судить об исправности схемы или характере неисправности в случае наличия таковой.

Математически предложенный способ контроля формализуется следующим образом. Пусть $f(x_1, \dots, x_n)$ — булева функция, а Σ_f — схема, ее реализующая. Пусть на схему воздействует источник неисправностей B , под действием которого Σ_f может перейти в неисправное состояние и реализовать одну из попарно неравных булевых функций $f_1(x_1, \dots, x_n), f_2(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$. Функции $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$ называются *функциями неисправности*. Множество наборов $T = \{\tilde{\alpha}_1, \dots, \tilde{\alpha}_p\}$ называется *проверяющим тестом* для схемы Σ_f относительно источника неисправностей B , если для любой функции неисправности $f_i(x_1, \dots, x_n)$, не равной исходной, в множестве T найдется набор, на котором функции $f(x_1, \dots, x_n)$ и $f_i(x_1, \dots, x_n)$ принимают разные значения. Если же в T для любых двух неравных функций из множества

$\{f(x_1, \dots, x_n), f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}$ существует набор, на котором значения функций различаются, то такое множество называется *диагностическим тестом* для схемы Σ_f относительно рассматриваемого источника неисправностей. Число наборов в тесте T называется его длиной, обозначается $l(T)$. Данная величина характеризует сложность тестирования. Тест минимальной длины называется *минимальным*.

Различают *единичные* и *полные* тесты. О единичных тестах говорят, если в схеме допускается всего одна неисправность (неисправен только один контакт в контактной схеме, один элемент в схеме из функциональных элементов и так далее). При изучении единичных тестов, как правило, рассматриваются только неизбыточные схемы, то есть такие, что при воздействии источника неисправностей реализуется функция, отличная от исходной [32]. Если допускается произвольное количество неисправностей, то говорят о *полных* тестах.

Очевидно, что в качестве теста всегда можно взять все булевы наборы длины n . Тогда получается тривиальный тест длины 2^n . Однако ясно, что во многих случаях такой тест будет являться избыточным. Например, в работе [43] показано, что для длины минимального диагностического теста T справедливы оценки: $\lceil \log(m+1) \rceil \leq l(T) \leq m$. Ясно, что верхняя оценка из данного неравенства будет справедлива и для проверяющих тестов. Поэтому ставится задача построения более коротких тестов для конкретных источников неисправностей B .

Сложность тестирования управляющих систем оценивается с помощью функции Шеннона. Определим $L(\Sigma_f, B) = \min_T l(T)$, где минимум берется по всем проверяющим (диагностическим) тестам для схемы Σ_f . Сложность тестирования булевой функции обозначим через $L(f, B) = \min_{\Sigma_f} (L(\Sigma_f, B))$, где минимум берется по всем схемам данного типа, реализующим булеву функцию f . В случае единичных тестов минимум берется по всем неизбыточным схемам, реали-

зующим f . Наконец, величина $L(n, B) = \max_{f \in P_2(n)} (L(f, B))$ называется функцией Шеннона длины проверяющего (диагностического) теста относительно источника неисправностей B .

Рассмотрим основные типы изучаемых неисправностей. Для контактных схем таковыми являются замыкание и обрыв контакта. В случае замыкания неисправный контакт проводит при любом значении соответствующей переменной, а в случае обрыва контакт не проводит ни при каком значении переменной. Для схем из функциональных элементов основные неисправности — это подстановка констант и инверсные неисправности. Причем различают неисправности на входах и на выходах функциональных элементов. В случае константных неисправностей на неисправные входы всегда поступают некоторые константы (в общем случае своя константа для каждого входа). В случае инверсных неисправностей значения неисправных входов всегда заменяются на противоположные. Если у функционального элемента произошла константная неисправность на выходе, то элемент вместо необходимой функции всегда реализует одну и ту же константу. При инверсной неисправности выхода элемент вместо необходимой функции реализует ее отрицание. Также рассматриваются неисправности входов схем. Пусть $x_{i_1}, \dots, x_{i_k}$ — переменные, соответствующие неисправным входам схемы, реализующей булеву функцию $f(x_1, \dots, x_n)$. Тогда вместо значений каждой из переменных $x_{i_1}, \dots, x_{i_k}$ на вход схемы поступают значения некоторых функций $\phi_1(x_1, \dots, x_n), \dots, \phi_k(x_1, \dots, x_n)$. Допустимые функции ϕ_j выбираются в зависимости от рассматриваемого источника неисправностей B . Ясно, что для данных неисправностей тест не зависит от вида схемы, реализующей рассматриваемую функцию, поэтому в случае тестирования относительно неисправностей входов схем будем говорить о тестах для булевых функций, а под функцией Шеннона длины проверяющего (диагностического) теста будем понимать максимум по всем булевым функциям длины минимального проверяющего (диагностическо-

го) теста для функции $f(x_1, \dots, x_n)$ относительно рассматриваемого источника неисправностей B .

Перечислим некоторые из имеющихся результатов в теории тестирования.

Х. А. Мадатян установил, что функция Шеннона длины полного диагностического теста для контактных схем относительно замыканий и обрывов контактов равна 2^n [11]. Н. П. Редькиным было получено, что при $n \geq 4$ функция Шеннона длины полного проверяющего теста относительно замыканий и обрывов контактов не превосходит $\frac{15}{16} \cdot 2^n$ [33]. Это означает, что тривиальный тест в данном случае не является минимальным. Также Н. П. Редькиным установлено, что функция Шеннона полного проверяющего теста при обрывах контактов равна $O(2^{\frac{n}{2}})$, полный проверяющий тест при замыкании контактов имеет длину не более, чем $O(2^{\frac{2n \log n}{1+2 \log n}})$ [34].

Для схем из функциональных элементов S. M. Reddy получил, что в базисе Жегалкина $\{xy, x \oplus y, 1\}$ любую булеву функцию можно реализовать схемой, допускающей единичный проверяющий тест относительно константных неисправностей на входах и выходах элементов длины не более, чем $n + 3$ [49]. Целый ряд результатов был получен Н. П. Редькиным. Им показано, что: 1) длина полного проверяющего теста в конечном базисе при константных неисправностях на выходах элементов ограничена сверху величиной $2(2^{\lceil \frac{n}{2} \rceil} + 2^{\lfloor \frac{n}{2} \rfloor} + n)$ [35]; 2) что в стандартном базисе $\{xy, x \vee y, \bar{x}\}$ длина полного диагностического теста относительно однотипных константных неисправностей на выходах элементов не превосходит по порядку $\sqrt{2^n}$ [36]; 3) что в стандартном базисе при однотипных константных неисправностях на выходах длина единичного диагностического теста не превосходит $2n + 1$ [37]; 4) что в любом конечном базисе произвольную булеву функцию можно реализовать схемой, допускающей единичный проверяющий тест длины 3 относительно инверсных неисправностей на выходах элементов [38]. С. В. Коваценок показал, что в базисе Жегалкина

при инверсных неисправностях на выходах элементов функция Шеннона длины единичного проверяющего теста равна 1 [7]. Ю. В. Бородина доказала, что в стандартном базисе функция Шеннона длины полного проверяющего теста относительно однотипных константных неисправностей на выходах элементов равна 2 [2]; что в базисе Жегалкина любую булеву функцию можно реализовать схемой, допускающей единичный проверяющий тест длины 1 относительно неисправностей типа 1 на выходах элементов [3]. В работе Ю. В. Бородиной и П. А. Бородина [4] установлено, что в базисе Жегалкина любую булеву функцию можно реализовать схемой, допускающей полный проверяющий тест длины 1 относительно неисправностей типа 0 на выходах элементов. Д. С. Романов установил, что в некотором базисе можно реализовать произвольную булеву функцию неизбыточной схемой, допускающей полный проверяющий тест при разнотипных константных неисправностях на выходах элементов длины 4 [39]; что в произвольном базисе булеву функцию, отличную от константы, можно реализовать неизбыточной схемой, допускающей единичный проверяющий тест при инверсных и произвольных константных неисправностях на выходах элементов [41].

По неисправностям входов схем В. Н. Носковым было установлено, что при $t \geq 7$ функция Шеннона длины проверяющего теста относительно подстановки констант равна $2n - 2t - 1$, если $n = 2^t + t + 1$, и $2n - 2t - 2$, если $2^t + t + 1 < n \leq 2^{t+1} + t + 1$ [27], а для почти всех функций длина проверяющего теста относительно подстановки констант асимптотически не менее $\frac{n}{2}$ и асимптотически не более $\frac{2n}{3}$ [27]. В. Н. Носковым доказано, что функция Шеннона длины полного диагностического теста относительно подстановки констант асимптотически не меньше, чем $\frac{2^{0.5n}}{2\sqrt{n}}$, и не больше, чем $2^{0.773n(1+O(\frac{\log_2 n}{n}))}$ [28]. Также В. Н. Носков рассматривал произвольные неисправности входов схем, при которых неисправны не более, чем k входов. Им показано, что для почти

всех булевых функций существует диагностический тест, логарифмической по общему числу входов длины [29]. Для этой же задачи Н. Н. Нурмеев доказал, что при случайном выборе множества наборов некоторой логарифмической по n длины это множество почти всегда образует диагностический тест [30].

Следующие результаты принадлежат Г. Р. Погосяну. Он показал, что функция Шеннона длины полного проверяющего теста относительно дизъюнктивных слипаний (а, следовательно, и конъюнктивных) в точности равна $n - 1$ [31], функция Шеннона длины полного проверяющего теста относительно инверсных неисправностей входов схем лежит в пределах от $n - 1$ до n [31]. Кроме того, Г. Р. Погосяном найдены оценки длин проверяющих тестов при некоторых смешанных неисправностях входов схем [8].

Н. И. Глазунов и А. П. Горяшко установили, что функция Шеннона длины проверяющего теста относительно единичных транспозиций переменных ограничена снизу числом $\frac{1}{4}n \log n$ [5]. Д. С. Романов показал, что длина теста относительно группы биекций на множестве переменных и их отрицаний ограничена сверху логарифмом мощности множества данной группы [50]. Отсюда и из результата Н. И. Глазунова и А. П. Горяшко следует, что функция Шеннона длины проверяющего теста относительно всевозможных биекций на множестве переменных имеет порядок $n \log n$. Д. С. Романов показал, что функция Шеннона длины диагностического теста относительно единичных транспозиций переменных асимптотически равна $\frac{n^2}{2}$ [40]. Также Д. С. Романову и И. В. Кузнецову принадлежат результаты исследований тестов относительно локальных k -кратных слипаний переменных в булевых функциях. При $n \rightarrow \infty$, $k \rightarrow \infty$, $n - k \rightarrow \infty$ ими установлено, что функция Шеннона длины полного проверяющего теста относительно локальных k -кратных слипаний переменных асимптотически равна $2^{k-1}(n - k)$, а функция Шеннона длины полного диагностического теста от-

носительно локальных k -кратных слипаний переменных асимптотически равна $2^k(n - k)$ [41, 51].

О. А. Долотова в своей диссертации получила ряд результатов, связанных с оценкой длин тестов относительно подстановки констант для функций из классов Поста. Результаты можно посмотреть в [8].

А. А. Икрамов в работе [6] установил, что для почти всех булевых функций существует проверяющий тест длины 1 относительно инверсии не более, чем одной переменной. Также в этой работе получен ряд оценок длин проверяющих тестов относительно смешанных неисправностей.

Из зарубежных работ близкой тематики можно отметить работу [47], в которой функционал, аналогичный функции Шеннона использовался как мера сложности обучения. В работе [53] были получены первые результаты по обнаружению константных неисправностей. Также можно отметить работы [52] и [46], относящиеся к теории вычислительного обучения, где постановка задачи близка к условным диагностическим тестам.

Настоящая диссертация состоит из введения, трех глав, заключения и списка литературы. Общий объем диссертации 83 страницы. Принята сквозная нумерация теорем, лемм и определений.

Опишем источники неисправностей, изучаемые в диссертации (формальные определения будут даны в соответствующих главах). Будем говорить, что в булевой функции $f(x_1, \dots, x_n)$ произошло Φ -слипание переменных $x_{i_1}, \dots, x_{i_k}$, если вместо каждой из этих переменных подставляется одна и та же функция из множества функций Φ , зависящая от $x_{i_1}, \dots, x_{i_k}$. Если все функции из Φ зависят от k переменных, то будем говорить о k -кратных слипаниях. Если в Φ -слипании участвуют подряд идущие переменные, будем говорить о локальных слипаниях. Если произошло несколько Φ -слипаний непересекающихся подмножеств переменных из $\{x_1, \dots, x_n\}$, то будем говорить о множественном Φ -слипании.

Приняты следующие обозначения источников неисправностей: $Q(\Phi)$ — Φ -слипания; $Q_k(\Phi)$ — k -кратные Φ -слипания; $MQ(\Phi)$ — множественные Φ -слипания; $MLQ_k(\Phi)$ — множественные локальные k -кратные Φ -слипания.

Помимо Φ -слипаний изучается вытеснение переменных функции $f(x_1, \dots, x_n)$. Переменные $x_1, \dots, x_n$ разбиваются на два непересекающихся подмножества вытесняемых и вытесняющих переменных. Вытеснение переменных заключается в том, что вместо каждой вытесняемой переменной подставляется произвольная функция, зависящая только от вытесняющих переменных.

Для описанных источников неисправностей исследуются проверяющие и диагностические тесты. Оцениваются функции Шеннона длин соответствующих тестов $L_{\text{detect}}(n, B)$, $L_{\text{diagn}}(n, B)$ (нижний индекс detect пишется у функции Шеннона длины проверяющего теста, а нижний индекс diagn у функции Шеннона длины диагностического теста), величина $M_{\text{detect}}(n, B)$, которая определяется аналогично функции Шеннона длины проверяющего теста, но максимум берется только по булевым функциям, существенно зависящим от всех своих переменных, а также $L_{\text{detect}}(f, B)$ — длина минимального проверяющего теста для функции $f(x_1, \dots, x_n)$.

В главе 1 рассматриваются проверяющие и диагностические тесты относительно линейных слипаний переменных в булевых функциях. Рассматриваются множества функций слипания Φ_{lin} , состоящее из всех линейных функций, и $\Phi_{\oplus}$, состоящее из линейных функций, существенно зависящих от всех своих переменных. Основные определения даются в разделе 1.1. В разделе 1.2 исследуется проверяющий тест относительно множественных линейных слипаний переменных. Основным результатом данного раздела является следующая теорема:

Теорема 1. При $n \rightarrow \infty$ верно следующее двойное неравенство:

$$\frac{n^2 - n}{2} \leq L_{\text{detect}}(n, MQ(\Phi_{\text{lin}})) \leq \frac{n^2}{2} + O(n\sqrt{n}).$$

В разделе 1.3 рассматриваются диагностические тесты относительно линейных слипаний, один из результатов доказан для случая общих слипаний, к которым относятся линейные. Основными результатами раздела являются следующие теоремы:

Теорема 2. Для функции Шеннона длины диагностического теста относительно множественных линейных слипаний верно следующее равенство:
 $L_{\text{diagn}}(n, MQ(\Phi_{\text{lin}})) = 2^n.$

Теорема 3. Пусть Φ — множество функций, такое, что $\forall k \exists g(y_1, \dots, y_k) \in \Phi$. Тогда для функции Шеннона $L_{\text{diagn}}(n, Q(\Phi))$ при некоторой вещественной положительной константе C_1 справедлива нижняя оценка: $L_{\text{diagn}}(n, Q(\Phi_{\text{lin}})) \geq C_1 \frac{2^{\frac{n}{2}}}{\sqrt[4]{n}}.$

Теорема 4. Для функции Шеннона $L_{\text{diagn}}(n, Q(\Phi))$ справедлива верхняя оценка $L_{\text{diagn}}(n, Q(\Phi_{\oplus})) \lesssim 2^{0.773n}.$

Раздел 1.4 первой главы посвящен тестам относительно локальных k -кратных линейных слипаний переменных в булевых функциях. Основными результатами раздела являются теоремы:

Теорема 5. При $n \rightarrow \infty$, $k \rightarrow \infty$, $k = o(n)$ для нечетных k верно: $M_{\text{detect}}(n, MLQ_k(\Phi_{\text{lin}})) \sim n$, для четных k верно:

$$4\frac{n}{k} \lesssim M_{\text{detect}}(n, MLQ_k(\Phi_{\text{lin}})) \lesssim 12\frac{n}{k}.$$

Теорема 6. При $n \rightarrow \infty$, $k \rightarrow \infty$, $k = o(n)$ верно: $L_{\text{detect}}(n, MLQ_k(\Phi_{\text{lin}})) \sim 2n$.

Теорема 7. При $n \rightarrow \infty$, $k \rightarrow \infty$, $k = o(n)$ верно: $L_{\text{diagn}}(n, LQ_k(\Phi_{\text{lin}})) \sim kn$.

В главе 2 изучаются тесты относительно монотонных симметрических слипаний переменных. В разделе 2.1 определяются рассматриваемые неисправности. В качестве множества Φ рассматриваются множества Φ_{ms} , состоящее из всевозможных монотонных симметрических функций, и множество $\Phi_{\vee}$, состоящее из всевозможных дизъюнкций. В разделе 2.2 изучается проверяющий тест относительно монотонных симметрических слипаний. Основным результатом раздела является теорема:

Теорема 8. При $n \rightarrow \infty$ имеет место неравенство:

$$2n \leq L_{\text{detect}}(n, MQ(\Phi_{\text{ms}})) \leq \frac{n^2}{2} + O(n \log n).$$

В разделе 2.3 исследуется диагностический тест относительно монотонных симметрических слипаний. В разделе доказана теорема:

Теорема 9. Имеет место равенство: $L_{\text{diagn}}(n, MQ(\Phi_{\text{ms}})) = 2^n$.

В разделе 2.4 рассматриваются диагностические тесты относительно дизъюнктивных слипаний. Основным результатом раздела является высокая нижняя оценка функции Шеннона длины диагностического теста относительно дизъюнктивных слипаний:

Теорема 10. Для функции Шеннона $L_{\text{diagn}}(n, Q(\Phi_{\vee}))$ при некоторой вещественной положительной константе C_2 справедлива нижняя оценка:
$$L_{\text{diagn}}(n, Q(\Phi_{\vee})) \geq C_2 \frac{2^n}{\sqrt{n}}.$$

В главе 3 изучается вытеснение переменных. В разделе 3.1 вводятся основные определения. В разделе 3.2 рассматриваются проверяющие тесты относительно вытеснения переменных. В следующей теореме формулируется оценка высокой степени точности длины данного теста:

Теорема 11. *Имеет место двойное неравенство*

$$2n - \log_2 n - 2 \log_2 \log_2 n + O(1) \leq L_{\text{detect}}(n, I) \leq 2n - \log_2 n + O(1).$$

Также найдена длина проверяющего теста относительно вытеснения переменных для почти всех булевых функций:

Теорема 12. *Для почти всех булевых функций $L_{\text{detect}}(f(x_1, \dots, x_n), I) = n + 1$.*

В разделе 3.3 исследуется диагностический тест относительно вытеснения переменных. Доказана следующая теорема:

Теорема 13. *Имеет место асимптотическое равенство: $L_{\text{diagn}}(n, I) \sim 2^n$.*

Результаты работы докладывались на следующих конференциях и семинарах:

- XVI Международная конференция «Проблемы теоретической кибернетики» (Нижний Новгород, 2011),
- XI Международный семинар «Дискретная математика и ее приложения» (Москва, 2012),
- Международная научная конференция студентов, аспирантов и молодых ученых «Ломоносов — 2013» (МГУ, 2013),
- IX Молодежная научная школа по дискретной математике и ее приложениям (Москва, 2013),
- Научная конференция «Тихоновские чтения» (Москва, 2013),
- Международная научная конференция студентов, аспирантов и молодых ученых «Ломоносов — 2014» (МГУ, 2014),
- XVII Международная конференция «Проблемы теоретической кибернетики» (Казань, 2014),
- Научная конференция «Тихоновские чтения» (Москва, 2014).

Основные результаты по теме диссертации изложены в 15 печатных изданиях [12–25, 48], из которых [12–17, 48] — в журналах из перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук. В работах [12, 17] Морозову Е. В. принадлежат все результаты, а Романову Д. С. — постановка задачи.

Глава 1

Тестирование булевых функций относительно линейных слипаний переменных

1.1 Основные определения и обозначения

Определим ряд источников неисправностей, связанных со слипаниями переменных. Пусть $f(x_1, \dots, x_n)$ — булева функция, Φ — множество булевых функций, такое что $\forall m \in \mathbb{N} \exists \phi(y_1, \dots, y_m) \in \Phi$. Тогда будем говорить, что в булевой функции $f(x_1, \dots, x_n)$ произошло Φ -слипание переменных $x_{i_1}, \dots, x_{i_k}$, если вместо исходной функции реализуется булева функция, полученная из нее подстановкой вместо каждой из переменных $x_{i_1}, \dots, x_{i_k}$ функции $\phi(x_{i_1}, \dots, x_{i_k})$, где функция $\phi \in \Phi$. Булеву функцию ϕ будем называть *функцией слипания*. Таким образом, получается источник неисправностей, называемый Φ -слипанием. Функциями неисправности являются булевы функции, получающиеся из исходной функции в результате всевозможных Φ -слипаний.

Если $i_1, \dots, i_k$ являются подряд идущими числами, то Φ -слипание будем называть *локальным*. Если допускается слипание ровно k переменных, то будем говорить о k -кратных слипаниях. Пусть $q \in \mathbb{N}$, $q \leq n$, $i_1, i_2, \dots, i_{j_1}, i_{j_1+1}, \dots, i_{j_2}, \dots, i_{j_{q-1}}, i_{j_{q-1}+1}, \dots, i_{j_q}$ — попарно различные натуральные

числа из отрезка $[1, n]$. Будем говорить, что в булевой функции $f(x_1, \dots, x_n)$ произошло множественное Φ -слипание переменных $x_{i_1}, \dots, x_{i_{j_1}}, \dots, x_{i_{j_{q-1}+1}}, \dots, x_{i_{j_q}}$, если вместо исходной функции реализуется булева функция, полученная из нее подстановкой вместо каждой из переменных $x_{i_1}, x_{i_2}, \dots, x_{i_{j_1}}$ функции $\phi_1(x_{i_1}, x_{i_2}, \dots, x_{i_{j_1}}) \in \Phi$, вместо каждой из переменных $x_{i_{j_1+1}}, \dots, x_{i_{j_2}}$ — функции $\phi_2(x_{i_{j_1+1}}, \dots, x_{i_{j_2}}) \in \Phi$ и так далее, вместо каждой из переменных $x_{i_{j_{q-1}+1}}, \dots, x_{i_{j_q}}$ — функции $\phi_q(x_{i_{j_{q-1}+1}}, \dots, x_{i_{j_q}}) \in \Phi$, функции $\phi_1, \dots, \phi_q$ также будем называть функциями слипания. Описанный источник неисправностей будем называть источником множественных Φ -слипаний. Функциями неисправности являются всевозможные булевы функции, получающиеся из $f(x_1, \dots, x_n)$ в результате множественных Φ -слипаний переменных при любых допустимых значениях чисел $q, i_1, i_2, \dots, i_{j_1}, i_{j_1+1}, \dots, i_{j_2}, \dots, i_{j_{q-1}}, i_{j_{q-1}+1}, \dots, i_{j_q}$. Если каждое из Φ -слипаний является локальным, то будем говорить о множественных локальных Φ -слипаниях. Как и во введении перечислим используемые обозначения изучаемых источников неисправностей: $Q(\Phi)$ — Φ -слипания; $Q_k(\Phi)$ — k -кратные Φ -слипания; $MQ(\Phi)$ — множественные Φ -слипания; $MLQ_k(\Phi)$ — множественные локальные k -кратные Φ -слипания.

Дадим еще несколько определений, которые будут часто использоваться в работе. Пусть дана функция $f(x_1, \dots, x_n)$. *Ребром направления i* или x_i будем называть два булевых n -мерных набора, отличающихся только в i -м разряде. Если на данных наборах функция $f(x_1, \dots, x_n)$ принимает разные значения, то данное ребро будет называть *правильным*. Множество наборов, содержащее хотя бы одно правильное ребро для каждой существенной переменной функции $f(x_1, \dots, x_n)$, будем называть *тестом существенности*. Ясно, что мощность теста существенности не превосходит $2n$ (в главе 3 будет дана более точная оценка). Совокупность наборов $\tilde{\alpha}$, для которых $|\tilde{\alpha}| = p$, назовем p -м *слоем* булева куба. Назовем функцию *симметрической*, если ее значения совпадают на любых

двух наборов, принадлежащих одному слою булева куба. Расстоянием Хэмминга $\rho(\tilde{\alpha}, \tilde{\beta})$ между булевыми наборами $\tilde{\alpha}$ и $\tilde{\beta}$ называется число разрядов, в которых эти наборы различаются.

1.2 Проверяющий тест относительно множественных линейных слипаний переменных

Первый результат данной главы устанавливает асимптотику функции Шеннона $L_{\text{detect}}(n, MQ(\Phi_{\text{lin}}))$. Предположим сначала некоторые определения и леммы, которые понадобятся в дальнейшем.

Определение 1. Проверяющей парой для переменных x_i, x_j , $i \neq j$, назовем пару наборов $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n), \tilde{\beta} = (\beta_1, \dots, \beta_n)$, обладающих следующими свойствами:

- $f(\alpha_1, \dots, \alpha_n) \neq f(\beta_1, \dots, \beta_n)$,
- $\alpha_k \neq \beta_k$ при $k \in \{i, j\}$,
- $\alpha_k = \beta_k$ в остальных случаях.

Введем бинарное отношение R_f на множестве переменных булевой функции $f(x_1, \dots, x_n)$ следующим образом. 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 $f(x_1, \dots, x_n)$ не существует проверяющей пары. Докажем лемму о данном бинарном отношении.

Лемма 1. Бинарное отношение R_f есть отношение эквивалентности.

Доказательство. Очевидно, данное отношение рефлексивно и симметрично. Докажем, что оно транзитивно. Пусть i, j, k — попарно различные натуральные числа, не превосходящие n . Тогда достаточно доказать, что если нет проверяющих пар для x_i, x_j и x_i, x_k , то нет проверяющей пары и для переменных

x_j, x_k . Будем считать, что $i = 1, j = 2, k = 3, \tilde{\gamma} = (\gamma_4, \gamma_5, \dots, \gamma_n)$ и выпишем соотношения, следующие из отсутствия проверяющих пар для x_1, x_2 и x_1, x_3 , из которых будет следовать требуемое утверждение: $f(1, 1, 0, \tilde{\gamma}) = f(0, 0, 0, \tilde{\gamma}) = f(1, 0, 1, \tilde{\gamma}) = f(0, 1, 1, \tilde{\gamma}), f(0, 0, 1, \tilde{\gamma}) = f(1, 1, 1, \tilde{\gamma}) = f(0, 1, 0, \tilde{\gamma}) = f(1, 0, 0, \tilde{\gamma})$. $\square$

Поскольку R_f является отношением эквивалентности, то оно разбивает множество переменных $x_1, \dots, x_n$ на непересекающиеся классы эквивалентности. Каждый класс эквивалентности будем называть *множеством линейности* переменных булевой функции $f(\tilde{x}^n)$ (смысл названия будет ясен позже). Для удобства будем далее считать, что переменные из одного множества линейности идут подряд. Для фиксированного $t \in N$ будем называть множество линейности A' t -мелким (соответственно t -крупным), если $|A'| \leq t$ (соответственно $|A'| > t$).

Лемма 2. Если $(\tilde{\alpha}, \tilde{\beta})$ — проверяющая пара для переменных x_i, x_j , то для любой переменной $x_k, k \in \{1, 2, \dots, n\} \setminus \{i, j\}$, существует набор $\tilde{\gamma}$, такой, что для x_i, x_k или x_j, x_k среди наборов $\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}$ есть проверяющая пара.

Доказательство. Пусть $i = 1, j = 2, k = 3$, наборы $(0, 0, 0, \alpha_4, \dots, \alpha_n), (1, 1, 0, \alpha_4, \dots, \alpha_n)$ образуют проверяющую пару для x_1, x_2 . Предположим, что невозможно добавить ровно один набор так, чтобы образовалась проверяющая пара для x_2, x_3 . Тогда получаем: $f(0, 0, 0, \alpha_4, \dots, \alpha_n) = f(0, 1, 1, \alpha_4, \dots, \alpha_n) = \sigma, f(1, 1, 0, \alpha_4, \dots, \alpha_n) = f(1, 0, 1, \alpha_4, \dots, \alpha_n) = \bar{\sigma}$. Видим, что $(0, 0, 0, \alpha_4, \dots, \alpha_n), (1, 0, 1, \alpha_4, \dots, \alpha_n)$ — проверяющая пара для x_1, x_3 . Аналогично рассматривается случай, когда невозможно добавить один набор, что получилась проверяющая пара для x_1, x_3 . Пусть $(0, 1, 0, \alpha_4, \dots, \alpha_n), (1, 0, 0, \alpha_4, \dots, \alpha_n)$ — проверяющая пара для x_1, x_2 . Действуя тем же образом, получаем: $f(0, 1, 0, \alpha_4, \dots, \alpha_n) = f(0, 0, 1, \alpha_4, \dots, \alpha_n) = \delta, f(1, 0, 0, \alpha_4, \dots, \alpha_n) = \bar{\delta}$. Видим, что $(1, 0, 0, \alpha_4, \dots, \alpha_n), (0, 0, 1, \alpha_4, \dots, \alpha_n)$ — проверяющая пара для x_1, x_3 . Ана-

логично рассматривается случай, когда невозможно добавить один набор, что получилась проверяющая пара для x_1, x_3 . $\square$

Следствие 1. Пусть переменная x_i принадлежит множеству линейности A' , а переменная x_j не принадлежит данному множеству. Если $(\tilde{\alpha}, \tilde{\beta})$ — проверяющая пара для x_i, x_j , то для любой переменной x_k из множества линейности A' существует набор $\tilde{\gamma}$, такой, что $(\tilde{\alpha}, \tilde{\gamma})$ или $(\tilde{\beta}, \tilde{\gamma})$ будет проверяющей парой для x_k, x_j .

Определение 2. Множество наборов называется основным проверяющим множеством для функции $f(x_1, \dots, x_n)$, если для каждой пары переменных x_i, x_j , не лежащих в одном множестве линейности функции $f(x_1, \dots, x_n)$, в этом множестве найдется проверяющая пара.

Лемма 3. Для любой булевой функции n переменных можно построить основное проверяющее множество мощностью не более, чем $\frac{n^2}{2} + O(n\sqrt{n})$.

Доказательство. Для доказательства данной леммы адаптируем метод, использованный в [40] для получения верхней оценки длины проверяющего теста относительно единичных транспозиций переменных в булевых функциях. Для некоторого натурального t определим множества переменных $Y_0, \dots, Y_{t-1}$ следующим образом: переменная x_k лежит в множестве Y_l , $l \in \{0, 1, \dots, t-1\}$, тогда и только тогда, когда $k = l \pmod{t}$. Положим $p = \left\lceil \frac{n}{t} \right\rceil$. Ясно, что $|Y_l| \leq p$.

Пусть T' — множество наборов, такое, что для каждого Y_l и каждой пары $x_i, x_j \in Y_l$, не лежащей в одном множестве линейности, в T' содержится соответствующая проверяющая пара наборов. Тогда $|T'| \leq tp(p-1)$. Для множества T' введем квадратную матрицу $Q(T') = [q_{ij}]_{n \times n}$ порядка n следующим образом:

$$q_{ij} = \begin{cases} 3, & \text{если верно, что } x_i R_f x_j, \\ 2, & \text{если проверяющая пара для } x_i, x_j \text{ содержится в множестве } T', \\ 1, & \text{если в множестве } T' \text{ нет проверяющей пары для } x_i, x_j, \\ & \text{но существует набор } \tilde{\gamma} \text{ такой, что проверяющая пара для } x_i, x_j \\ & \text{содержится в множестве } T' \cup \{\tilde{\gamma}\}, \\ 0, & \text{иначе.} \end{cases}$$

Обозначим через $\theta(T')$ число нулей в матрице $Q(T')$. Получим верхнюю оценку для $\theta(T')$.

Докажем, что если переменная x_k лежит в t -крупном множестве линейности A , то в матрице $Q(T')$ в строке и столбце, соответствующих x_k , не может быть нулей. Выберем произвольную переменную x_j , которая содержится в некотором Y_l , $l \in \{0, 1, \dots, t-1\}$. Если x_j лежит в том же множестве линейности A , что и x_k , тогда $q_{kj} = q_{jk} = 3$. Пусть x_j принадлежит другому множеству линейности, тогда в силу t -крупности множества линейности A в нем найдется переменная x_i , лежащая в Y_l . По построению T' в нем есть проверяющая пара для x_i, x_j . Тогда по следствию 1 получаем, что $q_{kj} = q_{jk} = 1$.

Далее рассмотрим случай, когда переменная x_k принадлежит t -мелкому множеству линейности A . Пусть $x_k \in Y_m$, $m \in \{0, 1, \dots, t-1\}$. Тогда в Y_m нет других переменных из множества линейности A в силу его t -мелкости. Покажем, что в столбце (следовательно, и строке) матрицы $Q(T')$, соответствующем переменной x_k , число нулей не превосходит $t-1$. По построению T' получаем, что для любой переменной $x_r \in Y_m$, отличной от x_k , $q_{rk} = q_{kr} = 2$. Пусть различные переменные x_i, x_j лежат в некотором множестве Y_l , ($m \neq l$), при этом $q_{ik} = q_{jk} = 0$. Из доказанного выше следует, что ни одна из них не лежит в t -крупном множестве линейности, а в одном t -мелком множестве линейности они не могут лежать в силу принадлежности Y_l и выбранному ранее порядку переменных. Значит, x_i, x_j лежат в разных t -мелких множествах линейности. Тогда

из леммы 2 следует, что в множестве T' лежит проверяющая пара для данных переменных и хотя бы одно из чисел q_{kj}, q_{ki} отлично от нуля. В итоге в столбце матрицы $Q(T')$, соответствующем переменной x_k , $x_k \in Y_m$, из t -мелкого множества линейности функции f , в строках переменных из Y_m нет нулей, а среди всех строк каждого из остальных множеств Y_l , $l \neq m$, нуль встречается не более, чем в одной строке.

Итак, $\theta(T') \leq n(t-1)$. Поскольку на главной диагонали матрицы стоят тройки, а каждой паре переменных x_i, x_j в матрице $Q(T')$ соответствуют две позиции q_{ij}, q_{ji} , получаем, что к T' достаточно добавить $\frac{n(n-p)}{2}$ (один набор на одну пару за исключением уже учтенных пар, т.е. лежащих в одном множестве Y_l , но в разных множествах линейности) и еще $\theta(T')$ наборов, чтобы получить искомое множество T'' . Таким образом,

$$|T''| \leq tp(p-1) + \theta(T') + \frac{n(n-p)}{2} \leq tp(p-1) + n(t-1) + \frac{n(n-p)}{2}.$$

Выбирая $t = \lceil \sqrt{n} \rceil$, получаем искомую оценку.

□

Лемма 4. Пусть ни для какой пары переменных функции $t(x_1, \dots, x_m)$ не существует проверяющей пары. Тогда $t(x_1, \dots, x_m)$ есть одна из четырех функций: 0 , 1 , $x_1 \oplus x_2 \oplus \dots \oplus x_m$, $x_1 \oplus x_2 \oplus \dots \oplus x_m \oplus 1$.

Доказательство. Наборы проверяющей пары отличаются в двух разрядах. Следовательно, если взять произвольный набор $\tilde{\alpha}$, у которого в i -й позиции стоит 0 , а в j -й позиции стоит 1 , и набор $\tilde{\beta}$, отличающийся от него ровно в этих разрядах, значения функции на данных наборах будут одинаковы. Получаем, что $t(x_1, \dots, x_m)$ — симметрическая функция. Кроме того, если в произвольном наборе $\tilde{\gamma}$ в позициях i и j стоят нули, а набор $\tilde{\delta}$ отличается от него ровно в этих двух разрядах, значения функции на данных наборах также будут одинаковы. Следовательно, функция $t(x_1, \dots, x_m)$ на всех четных слоях булева куба прини-

мает некоторое значение a , а на всех нечетных — некоторое значение b . Таких функций всего четыре: 0 , 1 , $x_1 \oplus x_2 \oplus \dots \oplus x_m$, $x_1 \oplus x_2 \oplus \dots \oplus x_m \oplus 1$ $\square$

Перейдем теперь к доказательству теоремы

Теорема 1 [13]. *При $n \rightarrow \infty$ верно следующее двойное неравенство:*

$$\frac{n^2 - n}{2} \leq L_{\text{detect}}(n, MQ(\Phi_{\text{lin}})) \leq \frac{n^2}{2} + O(n\sqrt{n}).$$

Доказательство. Рассмотрим сначала случай, когда функции слипания существенно зависят от всех своих переменных.

Включим в тест основное проверяющее множество наборов, полученное в лемме 3. Тогда если произошло слипание, при котором хотя бы две переменные из разных множеств линейности участвуют в одном слипании, на наборах из проверяющей пары для данных переменных (хотя бы одна такая пара содержится в построенном множестве) функция неисправности будет принимать равные значения, следовательно, неисправность будет обнаружена. Будем считать, что во всех последующих наборах, добавленных в тест, в позициях, соответствующих фиктивным переменным, стоят нули, если это не оговорено особо.

Следующим шагом добавим тест существенности в строящийся проверяющий тест. Это позволит обнаружить все слипания, при которых какая-то существенная переменная стала фиктивной.

Далее, пусть первые m_1 переменных образуют первое множество линейности функции $f(\tilde{x}^n)$, следующие $(m_2 - m_1)$ переменных — второе множество линейности и так далее, последние $(n - m_{r-1})$ переменных образуют r -е множество линейности.

Если $m_1 = 1$, то из не обнаруженных пока неисправностей в данном множестве линейности могла произойти только инверсия переменной x_1 . Это будет рассмотрено далее.

Пусть $m_1 \geq 2$. Зафиксируем значения всех переменных, кроме $x_1, \dots, x_{m_1}$, получим некоторую функцию от $x_1, \dots, x_{m_1}$. Поскольку у нее нет проверяющих пар ни для каких пар переменных, то можно применить лемму 4. Следовательно при любых зафиксированных значениях остальных переменных получается одна из четырех булевых функций: $0, 1, x_1 \oplus x_2 \oplus \dots \oplus x_{m_1}, x_1 \oplus x_2 \oplus \dots \oplus x_{m_1} \oplus 1$. Если в исходной функции все переменные $x_1, \dots, x_{m_1}$ фиктивны, то их слипания не влияют на реализуемую функцию. Если слипания переменных первого множества линейности таковы, что среди переменных $x_1, \dots, x_{m_1}$ появляются фиктивные, это будет обнаружено тестом существенности. Остается два варианта. В первом из них функция $x_1 \oplus x_2 \dots \oplus x_{m_1} \oplus c$ заменяется на $x_1 \oplus x_2 \dots \oplus x_{m_1} \oplus c \oplus 1$. Это эквивалентно инверсии любой переменной из первого множества линейности, например, переменной x_1 . Поэтому будем считать, что в этом варианте произошла инверсия x_1 , а остальные переменные $x_2, \dots, x_{m_1}$ не участвуют в слипаниях. Такой случай будет рассмотрен далее. Во втором варианте слипания таковы, что функция $x_1 \oplus x_2 \dots \oplus x_{m_1} \oplus c$ остается неизменной. Это не влияет на реализуемую функцию.

Аналогичные рассуждения можно провести для всех множеств линейности, содержащих не менее двух переменных.

Предположим, что поданы все наборы, входящие в тест на данный момент, но неисправность не была обнаружена. Необнаруженной неисправностью могут быть только инверсии некоторых переменных. В работе [31] установлено, что для тестирования $g(\tilde{y}^n)$ относительно инверсий переменных требуется не более, чем n наборов. Добавим эти наборы в тест.

На этом завершим рассмотрение функций слипания, существенно зависящих от всех своих переменных, и изучим остальные случаи. Если в результате слипания некоторая существенная переменная стала фиктивной, это обнаруживается на тесте существенности. В противном случае если в слипании участвует хо-

тя бы одна существенная переменная $f(\tilde{x}^n)$, то это эквивалентно некоторому слипанию с функцией слипания, существенно зависящей от всех своих переменных, которое было обнаружено ранее. Если слипаются только фиктивные переменные, то это не влияет на реализуемую функцию.

Подведем итог. Для всех пар переменных из разных множеств линейности в проверяющем множестве содержится проверяющая пара. Также добавлено линейное число наборов, составляющих тест на инверсии переменных и тест существенности. (В некоторых случаях данное число можно сократить, как будет показано в доказательстве теоремы 5, но здесь это не влияет на асимптотику и для простоты используется предложенный вариант). Отсюда следует верхняя оценка.

Докажем далее нижнюю оценку. Сузим класс неисправностей до слипаний двух переменных с функцией слипания $x \oplus y$, т.е. $\Phi = \{x \oplus y\}$. Рассмотрим функцию $f(x_1, \dots, x_n) = x_1 \vee x_2 \vee \dots \vee x_n$. Тогда для проверки слипания переменных x_i, x_j в тест необходимо добавить набор, у которого в позициях i и j стоят единицы, а в остальных нули, так как на других наборах получившаяся функция неисправности не отличается от исходной. Таким образом, для проверки всевозможных слипаний двух переменных необходимо C_n^2 наборов, откуда следует нижняя оценка. $\square$

Нетрудно видеть, что доказанная теорема справедлива и для линейных слипаний $Q(\Phi_{\text{lin}})$, поскольку при доказательстве нижней оценки все рассматриваемые функции неисправностей лежат в множестве $\Psi(f, Q(\Phi_{\text{lin}}))$.

1.3 Диагностические тесты относительно линейных слипаний переменных

В данной секции устанавливается точное значение функции Шеннона длины диагностического теста относительно множественных Φ -слипаний с множеством функций слипания Φ_{lin} и находятся оценки функции Шеннона длины диагностического теста относительно Φ -слипаний с множеством функций слипания $\Phi_{\oplus}$.

Теорема 2 [13]. *Для функции Шеннона длины диагностического теста относительно множественных линейных слипаний верно следующее равенство:*
$$L_{\text{diagn}}(n, MQ(\Phi_{\text{lin}})) = 2^n.$$

Доказательство. В работе [1] показывалось, что при инверсных неисправностях входов схем, реализующих булеву функцию $f(x_1, \dots, x_n) = x_1 \vee x_2 \vee \dots \vee x_n$, могут реализовываться всевозможные элементарные дизъюнкции n переменных. Поскольку отрицание переменной является линейной функцией, то множество функций неисправности для $f(x_1, \dots, x_n)$ также содержит всевозможные элементарные дизъюнкции n переменных. Можно получить тождественную единицу, подставив вместо переменных $f(x_1, \dots, x_n)$ единицы, которые также являются линейными функциями. А чтобы отличить каждую из элементарных дизъюнкций от тождественной единицы, потребуется 2^n наборов. Таким образом нижняя оценка функции Шеннона совпадает с множеством всех булевых n -мерных наборов, что завершает доказательство. $\square$

Далее докажем теорему, которая дает нижнюю оценку функции Шеннона длины диагностического теста относительно Φ -слипаний с практически любым множеством функций слипания Φ , в частности с $\Phi_{\oplus}$.

Теорема 3 [48]. *Пусть Φ — множество функций, такое, что $\forall k \exists g(y_1, \dots, y_k) \in \Phi$. Тогда для функции Шеннона $L_{\text{diagn}}(n, Q(\Phi))$ при*

некоторой вещественной положительной константе C_1 справедлива нижняя оценка: $L_{\text{diagn}}(n, Q(\Phi)) \geq C_1 \frac{2^{\frac{n}{2}}}{\sqrt[4]{n}}$.

Доказательство. Заметим, что если в элементарной конъюнкции $x_1^{\sigma_1} x_2^{\sigma_2} \dots x_m^{\sigma_m}$ произошло слипание, в котором участвуют переменные x_i, x_j , такие, что $\sigma_i \neq \sigma_j$, то данная конъюнкция обратится в ноль, поскольку вместо переменных, входящих в конъюнкцию с разными степенями, будет подставлена одна и та же величина. Воспользуемся данным наблюдением и построим функцию, схожую с использованной В. Н. Носковым [28] для константных неисправностей. Сначала будем предполагать, что $\forall k \exists g(y_1, \dots, y_k) \in \Phi$, не равная тождественному нулю. Опишем функцию, на которой достигается нижняя оценка:

$$h(x_1, \dots, x_n) = \bigvee_{\sigma_2 + \sigma_3 + \dots + \sigma_m = \lceil \frac{m}{2} \rceil - 1} x_1 x_2^{\sigma_2} \dots x_m^{\sigma_m} x_{m+1}^{\delta_1(\tilde{\sigma}^m)} \dots x_{n-m}^{\delta_{n-m}(\tilde{\sigma}^m)},$$

где векторы $\tilde{\delta}(\tilde{\sigma})$ выбираются так, что различным векторам $\tilde{\sigma}$ соответствуют разные $\tilde{\delta}(\tilde{\sigma})$ (m будет выбираться так, чтобы это было возможно). Найдем m , при котором число слагаемых в описанной ДНФ будет близко к максимальному.

Число всевозможных векторов $\tilde{\sigma}$, равное $C_{m-1}^{\lceil \frac{m}{2} \rceil - 1}$, тем больше, чем больше m . Число всевозможных векторов $\tilde{\delta}(\tilde{\sigma})$ равно 2^{n-m} , при этом должно выполняться неравенство $2^{n-m} \geq C_{m-1}^{\lceil \frac{m}{2} \rceil - 1}$ (правая часть неравенства соответствует числу требуемых векторов $(\sigma_2, \dots, \sigma_m)$). Используя известное асимптотическое равенство для биномиальных коэффициентов ($C_{2p}^p \sim \frac{2^{2p}}{\sqrt{\pi p}}$), при $m \rightarrow \infty$ получаем:

$$2^{n-m} \gtrsim a \frac{2^{m-1}}{\sqrt{\frac{\pi m}{2}}}, \text{ где } a \text{ — некоторая константа.}$$

Делим обе части неравенства на 2^{m-1} , логарифмируем, после чего получаем: $n - 2m + 1 \gtrsim \log \frac{a}{\sqrt{\frac{\pi m}{2}}}$ (здесь и далее логарифм берется по основанию 2).

Представим $m = \frac{n}{2} + t$, тогда $2t - 1 \lesssim \log \sqrt{\frac{n}{2} + t} - \log a \sqrt{\frac{2}{\pi}}$. Учтем, что $t \leq \frac{n}{2}$, отбросим последнее слагаемое, тогда получается, что $t \lesssim \frac{1}{4} \log n$. Отсюда

следует, что $2t - 1 \lesssim \log \sqrt{\frac{n}{2} + \frac{1}{4} \log n} - \log a \sqrt{\frac{2}{\pi}}$. При $t \sim \frac{1}{4} \log n$ данное неравенство превращается в асимптотическое равенство. Итак, получаем, что $m = \frac{n}{2} + \frac{1}{4} \log n + O(1)$.

Тождественный нуль получается из $h(x_1, \dots, x_n)$ слипанием всех переменных. Чтобы получить требуемую оценку, достаточно оценить снизу мощность множества наборов, отличающего нуль от других функций неисправности.

Предположим, что произошло слипание некоторых $\left\lceil \frac{m}{2} \right\rceil - 1$ переменных из $x_2, \dots, x_m$ и переменной x_1 , функция слипания — некоторая отличная от нуля функция. Во всех слагаемых выбранной ДНФ, кроме одного, степени хотя бы двух переменных из названных различны, следовательно только одно слагаемое может быть не равно тождественному нулю. Предположим, что данное слагаемое имеет вид: $x_1 x_2^{\sigma'_2} \dots x_m^{\sigma'_m} x_{m+1}^{\delta'_1} \dots x_n^{\delta'_{n-m}}$. Ясно, что оно не равно нулю только при $x_{m+1} = \delta'_1, \dots, x_n = \delta'_{n-m}$. Тогда каждому из рассматриваемых слипаний соответствуют различные вектора $\tilde{\delta}(\tilde{\sigma})$. Отсюда следует, что множества наборов, на которых соответствующие функции неисправности отличны от нуля, не пересекаются. Существование данных наборов обосновано тем, что среди функций слипания есть ненулевая функция.

Таким образом, чтобы отличить каждую из выбранных функций неисправности от тождественного нуля, потребуется столько же булевых наборов, сколько имеется функций неисправности. Их число равно $C_{m-1}^{\left\lceil \frac{m}{2} \right\rceil - 1}$. Поскольку можно выбрать $m = \frac{n}{2} + \frac{1}{4} \log n + O(1)$, снова воспользовавшись асимптотическим равенством для биномиальных коэффициентов, получаем требуемую оценку.

Если же при каком-то k в множестве Φ не будет необходимой отличной от нуля функции, то, рассуждая двойственным образом, снова получим требуемую нижнюю оценку. □

Перед доказательством следующей теоремы дадим несколько вспомогательных определений и лемм.

Через $f_{x_{i_1}, \dots, x_{i_k}}^{g(x_{i_1}, \dots, x_{i_k})}(x_1, \dots, x_n)$ будем обозначать функцию неисправности, получающуюся из $f(x_1, \dots, x_n)$ в результате слипания переменных $x_{i_1}, \dots, x_{i_k}$ с функцией слипания $g(x_{i_1}, \dots, x_{i_k})$. Для набора $\tilde{\alpha}$ через $|\tilde{\alpha}|$ обозначим число единиц в данном наборе.

Пусть $\tilde{\alpha}$ — некоторый n -мерный вектор, каждая компонента которого может принимать одно из значений: 0, 1 или 2. *Гранью* в кубе B^n будем называть множество булевых наборов этого куба, i -я компонента которых равна α_i , если α_i равна нулю или единице, и принимает произвольное значение, если $\alpha_i = 2$. Переменные, соответствующие двойкам в наборе $\tilde{\alpha}$, назовем *свободными переменными* грани, а их число — *размерностью* грани. Если в множестве булевых наборов Q содержится набор, принадлежащий некоторой грани в булевом кубе, будем говорить, что множество Q *протыкает* данную грань.

Пусть Z — подмножество множества переменных $\{x_1, \dots, x_n\}$, $\tilde{\alpha}, \tilde{\beta}$ — n -мерные булевы наборы. Будем обозначать: $\tilde{\alpha} =_Z \tilde{\beta}$, если разряды данных наборов, соответствующие переменным из Z , совпадают, $|\tilde{\alpha}|_Z = m$, если в разрядах набора $\tilde{\alpha}$ на местах переменных из Z стоит ровно m единиц.

Лемма 5. Пусть F_1 — множество функций неисправности, длина диагностического теста для которых равна l_1 , F_2 — множество функций неисправности, длина диагностического теста для которых равна l_2 . Тогда для множества функций неисправности $F = F_1 \cup F_2$ существует диагностический тест длины не более, чем $l_1 + l_2 + \min\{|F_1|, |F_2|\}$.

Доказательство. Пусть T_1 — диагностический тест длины l_1 для F_1 , T_2 — диагностический тест длины l_2 для F_2 . Положим $T' = T_1 \cup T_2$ и $|F_1| \leq |F_2|$. Тогда на множестве T' функции из F_1 отличены друг от друга, функции из F_2 отличены друг от друга, каждая функция из F_1 неотличима не более, чем от одной функ-

ции из F_2 . Первые два утверждения очевидны, покажем третье. Пусть это не так и некоторая функция $f_1 \in F_1$ неотличима от $f_2^1, f_2^2 \in F_2$, $f_2^1 \neq f_2^2$. В множестве T_2 , а следовательно и T' существует набор $\tilde{\alpha}$: $f_2^1(\tilde{\alpha}) \neq f_2^2(\tilde{\alpha})$. Тогда на данном наборе f_1 не равна одной из функций f_2^1, f_2^2 . Получаем противоречие. Отсюда следует, что для того, чтобы множество T' было диагностическим тестом для F , к нему достаточно добавить не более, чем $|F_1|$ наборов. $\square$

Зафиксируем некоторое число $k \geq 2$. По лемме о протыкании [26] можно построить множество наборов, протыкающее все грани булева куба размерности k , $R(k)$, такое, что $|R(k)| \leq (n+1)2^{n-k}$. Легко видеть, что данное множество является протыкающим и для всех граней размерности, большей k . Через $T_1(k)$ обозначим множество, состоящее из наборов множества $R(k)$ и всех наборов, находящихся от них на расстоянии, не большем 3. Тогда получаем: $|T_1(k)| \leq (n+1)(1 + C_n^1 + C_n^2 + C_n^3)2^{n-k} \lesssim \frac{n^4}{2}2^{n-k}$.

Лемма 6. Пусть $Z \subseteq X$, $|Z| \geq k$, $h(x_1, \dots, x_n)$ — булева функция, у которой ни для каких двух переменных из Z нет проверяющей пары. Тогда если для переменных x_r, x_s у $h(x_1, \dots, x_n)$ существуют проверяющие пары, то хотя бы одна проверяющая пара для них содержится в множестве $T_1(k)$.

Доказательство. Действительно, пусть $\tilde{\alpha}_1$ и $\tilde{\alpha}_2$ — проверяющая пара для переменных x_r и x_s . Множество наборов, совпадающих с $\tilde{\alpha}_1$ в разрядах, соответствующих переменным из $X \setminus Z$, образует грань в булевом кубе размерности $|Z| \geq k$, поэтому в $R(k)$ есть набор $\tilde{\beta}_1$, ее протыкающий.

Пусть $|\tilde{\beta}_1|_Z = |\tilde{\alpha}_1|_Z \pmod{2}$. Тогда $h(\tilde{\beta}_1) = h(\tilde{\alpha}_1)$. Это следует из леммы 4, поскольку, если зафиксировать значения переменных из множества $X \setminus Z$, будет реализовываться симметрическая функция, значения которой определяются только четностью числа единиц входного набора. Инвертируем в наборе $\tilde{\beta}_1$ разряды с номерами r и s , получим набор $\tilde{\beta}_2$. Рассуждая аналогично, получаем,

что $h(\tilde{\beta}_2) = h(\tilde{\alpha}_2)$, а следовательно, $\tilde{\beta}_1, \tilde{\beta}_2$ — проверяющая пара для переменных x_r, x_s функции $h(x_1, \dots, x_n)$. Набор $\tilde{\beta}_1$ лежит в $R(k)$, поэтому лежит и в $T_1(k)$. Набор $\tilde{\beta}_2$ находится от него на расстоянии 2, поэтому также лежит в $T_1(k)$.

Если $|\tilde{\beta}_1|_Z \neq |\tilde{\alpha}_1|_Z \pmod{2}$, выберем произвольную переменную x_j из $Z \setminus \{x_r \cup x_s\}$ и, инвертировав разряд j в наборе $\tilde{\beta}_1$, получим набор $\tilde{\beta}'_1$, а, инвертировав в $\tilde{\beta}'_1$ разряды r и s , получим $\tilde{\beta}'_2$. Выбранные наборы являются проверяющей парой для переменных x_r, x_s функции $h(x_1, \dots, x_n)$ (устанавливается аналогично). Данные наборы лежат в T' , поскольку $\rho(\tilde{\beta}_1, \tilde{\beta}'_1) = 1$, а $\rho(\tilde{\beta}_1, \tilde{\beta}'_2) = 3$. $\square$

Лемма 7. Пусть $Z \in X$, $|Z| \geq k$. Пусть у булевых функций $h_1(x_1, \dots, x_n)$, $h_2(x_1, \dots, x_n)$ нет проверяющих пар ни для каких двух переменных из Z и $h_1(x_1, \dots, x_n) \neq h_2(x_1, \dots, x_n)$. Тогда в множестве $T_1(k)$ существует набор, на котором данные функции неравны.

Доказательство. Пусть $h_1(\tilde{\alpha}) \neq h_2(\tilde{\alpha})$. Все наборы, отличающиеся от $\tilde{\alpha}$ в разрядах, соответствующих переменным из Z , образуют грань размерности $|Z|$, поэтому в множестве T содержится набор $\tilde{\beta}$, ее протыкающий. Допустим, что $|\tilde{\alpha}|_Z = |\tilde{\beta}|_Z \pmod{2}$. Тогда аналогично рассуждениям леммы 6 получаем: $h_1(\tilde{\beta}) = h_1(\tilde{\alpha}) \neq h_2(\tilde{\alpha}) = h_2(\tilde{\beta})$. Если же $|\tilde{\alpha}|_Z \neq |\tilde{\beta}|_Z \pmod{2}$, то вместо набора $\tilde{\beta}$ возьмем из множества $T_1(k)$ набор, соседний ему по какой-либо переменной из Z и, повторив проведенные рассуждения, получим, что данный набор различает функции $h_1(x_1, \dots, x_n)$ и $h_2(x_1, \dots, x_n)$. $\square$

Перейдем теперь к доказательству теоремы.

Теорема 4 [48]. Для функции Шеннона $L_{\text{diagn}}(n, Q(\Phi_{\oplus}))$ справедлива верхняя оценка $L_{\text{diagn}}(n, Q(\Phi_{\oplus})) \lesssim 2^{0.773n}$.

Доказательство. Поскольку доказывается асимптотическое неравенство, будем считать, что $n > 10$ (это необходимо, чтобы можно было правильным образом

выбрать k в конце доказательства). Разобьем доказательство на две части. На первом шаге выберем некоторое натуральное число $k \geq \left\lfloor \frac{n}{2} \right\rfloor$ и покажем, что множество наборов $T_1(k)$ различает все слияния кратности более, чем k .

Пусть $X' = \{x_{i_1}, \dots, x_{i_p}\}$ и $X'' = \{x_{j_1}, \dots, x_{j_q}\}$ — несовпадающие подмножества множества переменных $\{x_1, \dots, x_n\}$. Рассмотрим функции неисправности $f_{X'}^{g_1(x_{i_1}, \dots, x_{i_p})}$ и $f_{X''}^{g_2(x_{j_1}, \dots, x_{j_q})}$, где $g_1(x_{i_1}, \dots, x_{i_p}) \in \Phi_{\oplus}$ и $g_2(x_{j_1}, \dots, x_{j_q}) \in \Phi_{\oplus}$. Предположим, что $x_r, x_s \in X''$ и у функции $f_{X'}^{g_1(x_{i_1}, \dots, x_{i_p})}$ есть проверяющая пара для этих переменных. Очевидно, что ни для каких переменных из X' у функции $f_{X'}^{g_1(x_{i_1}, \dots, x_{i_p})}$ нет проверяющей пары, поэтому по лемме 6 получаем, что для переменных x_r, x_s у функции $f_{X'}^{g_1(x_{i_1}, \dots, x_{i_p})}$ есть проверяющая пара в множестве $T_1(k)$. На одном из наборов этой проверяющей пары функции различаются.

Если ни для какой пары переменных из X'' у функции $f_{X'}^{g_1(x_{i_1}, \dots, x_{i_p})}$ нет проверяющей пары, то мы можем применить лемму 7, взяв X'' в качестве множества Z . Тогда если выбранные функции неисправности различаются, в $T_1(k)$ имеется набор, на котором они неравны.

Рассмотрим теперь слияния кратности не выше k . Число всевозможных функций неисправности не превышает $2(1 + C_n^1 + \dots + C_n^k) \leq 2kC_n^k$. Из тривиальной верхней оценки длины диагностического теста следует, что мощность множества наборов $T_2(k)$, различающего выбранные функции неисправностей, ограничена сверху числом $2kC_n^k - 1$.

Таким образом, все слияния кратности выше k отличены друг от друга, и все слияния кратности не выше k различены между собой. Если T — искомый диагностический тест, то, применяя лемму 5, получаем верхнюю оценку мощности множества T : $|T| \leq 2kC_n^k + \frac{n^4}{2}2^{n-k} + \min(2kC_n^k, 2^{n+1} - 2kC_n^k)$.

Введем функцию $H(a) = -a \log a - (1 - a) \log(1 - a)$. Применяя известное неравенство $C_n^r < 2^{nH(\frac{r}{n})}$ [42], выбирая $k = \lceil 0,2271n \rceil$ и пользуясь таблицей значений для функции $H(a)$, получаем, что при $n \rightarrow \infty$ верно:

$$|T| \leq 2kC_n^k + \frac{n^4}{2}2^{n-k} + \min \{2kC_n^k, 2^{n+1} - 2kC_n^k\} \lesssim n2^{0.77293n} + \frac{1}{2}n^42^{0.7729n} + n2^{0.77293n} \lesssim 2^{0.773n}. \quad \square$$

1.4 Локальные k -кратные слипания переменных

В данном разделе исследуются проверяющие тесты относительно локальных k -кратных линейных слипаний, в том числе множественных, а также диагностические тесты относительно локальных k -кратных линейных слипаний.

Начнем с проверяющих тестов. Нетрудно видеть, что можно найти один набор и добавить его к проверяющей паре для x_i, x_j так, чтобы среди данных трех наборов содержалось правильное ребро направления x_i или x_j . Если обе переменные существенны, то добавим к ним правильное ребро направления оставшейся переменной, получим *проверяющую пятерку*.

Множество переменных $x_i, \dots, x_{i+p}$ 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 $f(x_1, \dots, x_n)$ все переменные существенны, линейно-фиктивно нерасширяемое множество будем для простоты называть *линейно нерасширяемым* множеством.

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

Лемма 8. *При $n \rightarrow \infty, k \rightarrow \infty, k = o(n)$ для функции $f(x_1, \dots, x_n)$ можно построить локальное проверяющее множество $S_k(f)$ мощностью асимптотически не более, чем $15 \cdot \frac{n}{k}$. Если же $f(x_1, \dots, n)$ существенно зависит от всех*

своих переменных, то можно построить $S_k(f)$ мощностью асимптотически не более, чем $10 \cdot \frac{n}{k}$.

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

Пусть $i_1, i_1 \geq 1$ — наименьшее число такое, что $x_{i_1}, \dots, x_{i_1+k-1}$ не лежат в одном линейно-фиктивно нерасширяемом множестве. Выберем максимальные p_1, q_1 такие, что $i_1 \leq p_1 < q_1 \leq i_1 + k - 1$ и для переменных x_{p_1}, x_{q_1} существует проверяющая пара. Добавим для них проверяющую пару в $S_k(f)$. Выберем $i_2, i_2 \geq p_1 + 1$, — наименьшее число, такое, что $x_{i_2}, \dots, x_{i_2+k-1}$ не лежат в одном линейно-фиктивно нерасширяемом множестве (при меньших i_2 проверяющая пара для каких-то переменных из $x_{i_2}, \dots, x_{i_2+k-1}$ 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 $i_2 \leq p_2 < q_2 \leq i_2 + k - 1$. 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 следующему шагу, на котором $i_3 \geq p_2 + 1$, а q_3 будет больше $i_2 + k - 1$. 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 была добавлена. И так далее. Получаем, что на j -м шаге добавляется проверяющая пара для некоторых переменных из множества $x_{i_j}, \dots, x_{i_j+k-1}$. Причем $i_j \geq p_{j-1} + 1, q_j > i_{j-1} + k - 1$. Также легко видеть, что $p_j \geq q_{j-1}$. Тогда $q_j > i_{j-1} + k - 1 \geq p_{j-2} + k \geq q_{j-3} + k$. Отсюда получается, что при указанных условиях на n и k число проверяющих пар асимптотически не более $3 \cdot \frac{n}{k}$. По построению получается, что для каждой k подряд идущих переменных, не принадлежащих одному линейно-фиктивно нерасширяемому множеству, в $S_k(f)$ была добавлена проверяющая пара. Доба-

вим для каждой пары три набора так, чтобы получалась проверяющая пятерка. Отсюда следует, что $|S_k(f)| \lesssim 15 \cdot \frac{n}{k}$.

Теперь пусть $f(x_1, \dots, x_n)$ существенно зависит от всех своих переменных. Заметим, что в этом случае $q_j = i_j + k - 1$. Действительно, пусть среди переменных $x_{i_j}, \dots, x_{i_j+k-1}$ не все переменные принадлежат одному множеству линейности (определено в разделе 1.2). 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 $x_{i_j+t+1}, \dots, x_{i_j+k-1}$ принадлежат одному множеству линейности. Тогда $p_j = i_j + t$, $q_j = i_j + k - 1$. Тогда неравенства из предыдущего абзаца преобразуются в: $i_j \geq p_{j_1} + 1$, $p_j \geq q_{j-1}$, $q_j = i_j + k - 1$. Получаем: $q_j = i_j + k - 1 \geq p_{j-1} + k \geq q_{j-2} + k$. Отсюда следует, что при указанных условиях на n и k число проверяющих пар асимптотически не более $2 \cdot \frac{n}{k}$. Тогда строим по ним $S_k(f)$, $|S_k(f)| \lesssim 10 \cdot \frac{n}{k}$.

□

Лемма 9. Пусть $g(x_1, \dots, x_m)$ — некоторая линейная функция m переменных, $A = \{\tilde{\alpha}_1, \dots, \tilde{\alpha}_m\}$ — множество булевых наборов. Тогда существует отличная от g линейная функция $h(x_1, \dots, x_m)$, равная функции g на всех наборах множества A .

Доказательство. Пусть набор $\tilde{\alpha}_i = (\alpha_1^i, \dots, \alpha_m^i)$, $g(\tilde{\alpha}_i) = a_i$. Запишем систему линейных уравнений относительно возможных коэффициентов линейной функции $c_1, \dots, c_{m+1}$:

$$\begin{cases} c_1 \alpha_1^i \oplus \dots \oplus c_m \alpha_m^i \oplus c_{m+1} = a_1, \\ \dots, \\ c_1 \alpha_1^i \oplus \dots \oplus c_m \alpha_m^i \oplus c_{m+1} = a_m. \end{cases}$$

Система совместна в силу существования функции $g(x_1, \dots, x_m)$. Но поскольку число неизвестных меньше числа уравнений, получаем, что существует как

минимум 2 решения данной системы. Одно определяет функцию $g(x_1, \dots, x_m)$, другое — функцию $h(x_1, \dots, x_m)$. $\square$

Лемма 10. Пусть $g(x_1, \dots, x_m) = x_1 \dots x_m$, $m \geq 2$, $A = \{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$ — произвольное множество булевых наборов. Тогда существует линейная функция $h(x_1, \dots, x_m)$ m переменных, которая равна $g(x_1, \dots, x_m)$ на A .

Доказательство. Пусть на наборах $\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\}$ функция $g(x_1, \dots, x_m)$ равна a_1, a_2, a_3 соответственно. Запишем систему линейных уравнений относительно возможных коэффициентов линейной функции $c_1, \dots, c_{m+1}$:

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

Достаточно показать, что ранг основной матрицы системы равен трем. Действительно, нулевых строк у данной матрицы нет, так как $(m+1)$ -й элемент любой строки равен 1. Если сложить любые две строки этой матрицы, 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 (так как коэффициент перед c_{m+1} во всех строках матрицы равен единице.). Поэтому строки основной матрицы линейно независимы, ее ранг равен трем, система имеет решение, следовательно задает некоторую линейную функцию $h(x_1, \dots, x_m)$, удовлетворяющую условию леммы. $\square$

Через $\delta(\alpha_1, \dots, \alpha_m)$ обозначим $\sum_{i=0}^{m-1} \alpha_{m-i} 2^i$. Введем функцию:

$$\mu_{r,s}(x_1, \dots, x_r, y_1, \dots, y_s) = \bigvee_{\sigma_1, \dots, \sigma_r: \delta(\sigma_1, \dots, \sigma_r) < s} x_1^{\sigma_1} x_2^{\sigma_2} \dots x_r^{\sigma_r} y_{\delta(\sigma_1, \dots, \sigma_r)+1}.$$

Переменные $x_1, \dots, x_r$ назовем адресными, переменные $y_1, \dots, y_s$ — информационными. Эта функция будет использоваться при получении нижних оценок.

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

Теорема 5 [17]. При $n \rightarrow \infty$, $k \rightarrow \infty$, $k = o(n)$ для нечетных k верно:
 $M_{\text{detect}}(n, MLQ_k(\Phi_{\text{lin}})) \sim n$, для четных k верно:

$$4 \cdot \frac{n}{k} \lesssim M_{\text{detect}}(n, MLQ_k(\Phi_{\text{lin}})) \lesssim 12 \cdot \frac{n}{k}.$$

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

Добавим в T_1^* и T_2^* локальное проверяющее множество $S_k(f)$ для функции $f(x_1, \dots, x_n)$.

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 же хоть одна из этих переменных стала фиктивна, в $S_k(f)$ есть правильное ребро данного направления, на одном из наборов которого неисправность обнаружится.

Пусть теперь переменные $x_i, \dots, x_{i+r}$, $r \geq k - 1$, составляют линейно нерасширяемое множество. Зафиксируем значения остальных переменных. Тогда по лемме 4 будет реализовываться одна из четырех линейных функций. Поскольку все переменные f существенны, существуют $\beta_1, \dots, \beta_{i-1}, \beta_{i+r+1}, \dots, \beta_n$ такие, что $f(\beta_1, \dots, \beta_{i-1}, x_i, \dots, x_{i+r}, \beta_{i+r+1}, \dots, \beta_n) = x_i \oplus \dots \oplus x_{i+r} \oplus d$, где $d = d(\beta_1, \dots, \beta_{i-1}, \beta_{i+r+1}, \dots, \beta_n) \in \{0, 1\}$. Если k четное, то при слипании любых подряд идущих переменных из $x_i, \dots, x_{i+r}$ эти переменные станут фиктивными, так как вместо каждой из них подставляется одна и та же величина. В таком случае достаточно добавить в тест правильные ребра для переменных $x_{i+k}, x_{i+2k}, \dots, x_{i+\lfloor \frac{r-i}{k} \rfloor k}$, и неисправность будет проверена. Если же k — нечетное, добавим в тест n -мерный набор $(\beta_1, \dots, \beta_{i-1}, 1, \dots, 1, \beta_{i+r+1}, \dots, \beta_n)$ и все соседние ему наборы по переменным $x_i, \dots, x_{i+r}$. Это обнаружит слипания любых k подряд идущих переменных из $x_i, \dots, x_{i+r}$, если у соответствующей функции сли-

пания есть фиктивные переменные (добавлены правильные ребра направлений $x_i, \dots, x_{i+r}$). 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 четное, проверяющий тест построен. На каждые k переменных линейно-нерасширяемого множества приходится 2 набора. Тогда всего в T_2^* было добавлено асимптотически не более, чем $12 \cdot \frac{n}{k}$.

В случае нечетного k непроверенным остается только случай, когда произошло несколько слипаний. Причем если переменные $x_i, \dots, x_{i+k-1}$ из одного множества линейности составляют один блок слипания, то функция слипания равна $x_i \oplus \dots \oplus x_{i+k-1} \oplus 1$. Пусть $X_1, \dots, X_u$ — множества линейности функции $f(x_1, \dots, x_n)$. Заметим, что они необязательно состоят из подряд идущих переменных. Представим функцию $f(x_1, \dots, x_n)$ как суперпозицию некоторой функции $g(y_1, \dots, y_u)$ и линейных функций вида $l(z_1, \dots, z_v) = z_1 \oplus z_2 \oplus \dots \oplus z_v$.

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

$f(x_1, x_2, \dots, x_7) = (x_1 \oplus x_2 \oplus x_3)(x_4 \oplus x_5 \oplus x_6)x_7 \vee (x_1 \oplus x_2 \oplus x_3 \oplus 1)(x_4 \oplus x_5 \oplus x_6 \oplus 1)\bar{x}_7$. Тогда получаем суперпозицию $g(y_1, y_2, y_3) = y_1 y_2 y_3 \vee (y_1 \oplus 1)(y_2 \oplus 1)\bar{y}_3$ из функций $y_1(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$, $y_2(x_4, x_5, x_6) = x_4 \oplus x_5 \oplus x_6$, $y_3(x_7) = x_7$.

Если среди переменных множества линейности функции f произошло одно или несколько слипаний рассматриваемого типа, это либо не меняет исходную функцию, либо эквивалентно инверсии соответствующей переменной функции g . Для $g(y_1, \dots, y_u)$ можно построить полный проверяющий тест относительно инверсий переменных мощностью не более, чем u [31]. 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 $\left\lfloor \frac{n}{k} \right\rfloor$. Если суммарное число переменных в них равно s , то число добавленных в тест наборов не превосходит $(10 \cdot \left\lceil \frac{n}{k} \right\rceil) + (s + \left\lfloor \frac{n}{k} \right\rfloor) + u$. Первое слагаемое соответствует $S_k(f)$, второе — правильным ребрам для переменных линейно нерасширяемых множеств, третье — тесту на инверсии. Поскольку любое линейно нерасширяемое множество целиком лежит в некотором множестве линейности, то легко видеть, что $u \leq n - s + \left\lfloor \frac{n}{k} \right\rfloor$. Получаем итоговую оценку $|T_1^*| \leq n + 12 \cdot \left\lfloor \frac{n}{k} \right\rfloor$.

Перейдем к нижней оценке. Оценим снизу $M_{\text{detect}}(n, MLQ_k(\Phi_{lin}))$ при нечетном k . Обозначим $r = \left\lceil \log_2 \frac{n}{k} \right\rceil$, $s = \left\lfloor \frac{n-r}{k} \right\rfloor$. Рассмотрим функцию $f(x_1, \dots, x_n) = x_{r+sk+1} \dots x_n \mu_{r,s}(x_1, \dots, x_r, x_{r+1} \oplus x_{r+2} \dots \oplus x_{r+k}, x_{r+k+1} \oplus \dots \oplus x_{r+2k}, \dots, x_{r+(s-1)k+1} \oplus \dots \oplus x_{r+sk})$. На всех рассматриваемых далее наборах будем считать переменные $x_{r+sk+1}, \dots, x_n$ равными единице, потому что в противном случае функция будет равна единице и слипания остальных переменных будут необнаруживаемы. Обнаружить слипание переменных $x_{r+1}, \dots, x_{r+k}$ можно только при одном наборе значений адресных переменных. Зафиксировав таким образом $x_1, \dots, x_r$, получаем, что в исправном состоянии должна реализовываться функция $x_{r+1} \oplus x_{r+2} \oplus \dots \oplus x_{r+k}$. В случае переменных слипания $x_{r+1}, x_{r+2}, \dots, x_{r+k}$ может реализовываться любая линейная функция. Чтобы отличить верную линейную функцию от остальных возможных по лемме 9 необходимо не менее, чем $(k+1)$ наборов. Далее тем же способом рассматривается

слипание следующих k переменных и так далее. В итоге получаем, что при $n \rightarrow \infty, k \rightarrow \infty, k = o(n)$ число наборов проверяющего теста асимптотически не меньше n .

Теперь оценим снизу $M_{\text{detect}}(n, MLQ_k(\Phi_{\text{lin}}))$ при четном k . Доказательство проводится аналогично случаю с нечетным k , только в качестве информационных переменных подается s конъюнкций: $x_{r+1} \& x_{r+2} \& \dots \& x_{r+k}, \dots, x_{r+(s-1)k+1} \& \dots \& x_{r+sk}$. Используется лемма 10 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 $n \rightarrow \infty, k \rightarrow \infty, k = o(n)$ число информационных переменных асимптотически равно $\frac{n}{k}$, для каждой конъюнкции необходимо 4 набора. $\square$

Теорема 6 [17]. При $n \rightarrow \infty, k \rightarrow \infty, k = o(n)$ верна асимптотическая оценка: $L(n, MLQ_k(\Phi_{\text{lin}})) \sim 2n$.

Доказательство. Снова докажем сначала верхнюю оценку. Возьмем произвольную функцию $f(x_1, \dots, x_n)$ и будем строить для нее проверяющий тест T . Первым действием добавим в T локальное проверяющее множество $S_k(f)$.

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

лось в результате слипания, на одном из добавленных наборов это обнаружится. Остается только неисправность, при которой вместо функции $x_{i_1} \oplus \dots \oplus x_{i_p} \oplus d$ реализуется ее отрицание. В зависимости от слипаний остальных переменных это может привести либо к инверсии некоторого множества линейности, либо не изменить функцию. Подобная неисправность будет обнаружена на последнем шаге аналогично доказательству в предыдущей теореме.

Основное отличие данного доказательства в том, что следующее рассматриваемое линейно-фиктивно нерасширяемое множество может начинаться с x_{i_p+1} , а не x_{i_r} (оно не может начинаться с переменной еще 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-фиктивных нерасширяемых множеств мощностью не менее, чем k , можно оценить сверху через $2 \cdot \frac{n}{k}$.

Необнаруженными остались только неисправности, связанные с инверсиями множеств линейности. Их проверяем тестом на инверсии описанным в предыдущей теореме способом.

Теперь подсчитаем число добавленных в T наборов. Пусть суммарное число переменных в линейно-фиктивно нерасширяемых множествах мощностью не менее k равно s , число самих подмножеств равно t . Тогда число наборов можно оценить сверху через $(|S_k(f)|) + (2s + t - t) + (n - s + t) \leq 2n + 17 \cdot \frac{n}{k}$. Смысл первого слагаемого ясен. Во втором слагаемом прибавляется t , так как каждому линейно-фиктивному множеству соответствует набор, на котором все переменные множества равны единице. Во втором слагаемом далее 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. Этот набор не был учтен ранее. Третье слагаемое получается аналогично предыдущей теореме.

Перейдем к нижней оценке. Обозначим $r = \left\lceil \log_2 \frac{2n}{k+1} \right\rceil$, $s = 2 \left\lfloor \frac{n-r}{k+1} \right\rfloor$. Рассмотрим функцию $f(x_1, \dots, x_n) = \mu_{r,s}(x_1, \dots, x_r, x_{r+1}, x_{r+k+1}, x_{r+k+2}, x_{r+2k+2}, x_{r+2k+3}, \dots, x_{r+\frac{s}{2}(k+1)})$. Рассмотрим слипания переменных $x_{r+1}, \dots, x_{r+k}$. Ясно, что при их слипании значение функции может поменяться только при одном наборе $\sigma_1, \dots, \sigma_r$ значений адресных переменных. Зафиксировав таким образом $x_1, \dots, x_r$, получаем, что в исправном состоянии должна реализовываться функция x_{r+1} . В неисправном же может реализовываться любая линейная функция переменных $x_{r+1}, \dots, x_{r+k}$. По лемме 9 необходимо как минимум $(k+1)$ наборов, чтобы отличить линейную функцию x_{r+1} от остальных возможных. Обнаружить слипание переменных $x_{r+2}, \dots, x_{r+k+1}$ можно только при другом наборе адресных переменных, и на это также потребуется $(k+1)$ наборов. И так далее, чтобы обнаружить слипание каждой информационной переменной с соседними ей $(k-1)$ фиктивными переменными необходимо брать ранее не использованные $(k+1)$ наборов. Причем у каждой информационной переменной будет $(k-1)$ фиктивных переменных, соседних слева, и $(k-1)$ фиктивных переменных, соседних справа. При $n \rightarrow \infty$, $k \rightarrow \infty$, $k = o(n)$ число информационных переменных асимптотически равно $2 \cdot \frac{n}{k+1}$, следовательно число наборов проверяющего теста подобной функции асимптотически не меньше $2n$. $\square$

Заметим, что в работе автора и Д. С. Романова [12] также изучались проверяющие тесты относительно локальных k -кратных линейных слипаний, однако были получены менее точные оценки.

Теперь перейдем к диагностическим тестам. Через $M(\Phi)$ обозначим матрицу, столбцами которой являются булевы функции из Φ , а через $M^+(\Phi)$ — матрицу, получающуюся из $M(\Phi)$ приписыванием снизу строки из единиц. Через $w(M)$ обозначим ранг матрицы M , а через $l(M)$ — длину минимального диагностического теста для матрицы M (под диагностическим тестом для матрицы M понимается такое множество номеров строк матрицы M , что если столбцы матрицы с номерами j_1 и j_2 не являются равными, то в данном множестве существует такое число i , что $M(i, j_1) \neq M(i, j_2)$, а под длиной диагностического теста для матрицы понимается его мощность). В работе Д. С. Романова [51] доказано, что если функции слияния из Φ формально зависят от k переменных и $2 \leq k \leq n$, а число функций слияния лежит в множестве $\{1, 2, \dots, 2^{2^k}\}$, то $(l(M(\Phi)) - 1)(n - k + 1) \leq L_{\text{diagn}}(n, LQ_k(\Phi)) \leq w(M^+(\Phi))(n - k + 1) + 1$.

Применим данные результаты к множеству функций слияния Φ_{lin} . Сначала заметим, что $w(M^+(\Phi_{\text{lin}})) \leq k + 2$. Поскольку ранг матрицы равен максимальному числу ее линейно независимых столбцов, будем рассматривать столбцы $M^+(\Phi_{\text{lin}})$. Каждый столбец исходной матрицы $M(\Phi_{\text{lin}})$ соответствует некоторой линейной функции. Поэтому любой столбец этой матрицы является суммой некоторых столбцов из $(k + 1)$ столбцов, соответствующих линейным функциям $\{1, y_1, \dots, y_k\}$. Без ограничения общности будем считать, что это столбцы с номерами $1, 2, \dots, k + 1$. Пусть, например, j -й столбец есть сумма столбцов с номерами $j_1, \dots, j_q$, где $1 \leq j_1 < \dots < j_q \leq k + 1$. Тогда если q нечетное число, то j -й столбец матрицы $M^+(\Phi_{\text{lin}})$ есть сумма столбцов с номерами $j_1, \dots, j_q$. Если же q четное, то j -й столбец $M^+(\Phi_{\text{lin}})$ есть сумма столбцов с номерами $j_1, \dots, j_q$ и столбца, соответствующего нулевой функции. Получаем, что ранг матрицы $M^+(\Phi_{\text{lin}})$ не превосходит $k + 2$ (нетрудно показать, что на самом деле имеет место точное равенство). Неравенство $l(M(\Phi_{\text{lin}})) \geq k + 1$ следует из того, что в матрице $M(\Phi_{\text{lin}})$ ровно 2^{k+1} различных между собой столбцов, то есть диагно-

стический тест не может быть меньше $k + 1$ [10]. Нетрудно видеть, что существует диагностический тест такой длины. Также заметим, что число функций неисправности в Φ_{lin} есть 2^{k+1} , каждая функция неисправности формально зависит от k переменных. Из всего вышесказанного получается следующая оценка функции Шеннона длины диагностического теста относительно локальных k -кратных линейных слипаний:

Теорема 7 [12]. *При $n \rightarrow \infty$, $k \rightarrow \infty$, $k = o(n)$ верна асимптотическая оценка: $L_{\text{diagn}}(n, LQ_k(\Phi_{\text{lin}})) \sim kn$.*

Глава 2

Тестирование булевых функций относительно монотонных симметрических слипаний переменных

2.1 Основные определения и обозначения

В данной главе изучаются Φ —слипания переменных, при которых функции слипания являются монотонными симметрическими. Рассматриваются множество функций слипания Φ_{ms} , состоящее из всевозможных монотонных симметрических функций, и более узкое множество функций слипания $\Phi_{\vee}$, состоящее из всевозможных дизъюнкций. Далее под монотонными симметрическими слипаниями будем понимать Φ -слипания, при которых $\phi \in \Phi_{\text{ms}}$, а под дизъюнктивными слипаниями — Φ -слипания, при которых $\phi \in \Phi_{\vee}$.

Дизъюнктивные слипания впервые изучались Г. Р. Погосяном в [31]. Им было доказано, что функция Шеннона длины проверяющего теста относительно множественных дизъюнктивных слипаний равна $n - 1$.

В настоящей главе получены нетривиальные верхняя и нижняя оценки функции Шеннона длины проверяющего теста относительно множественных монотонных симметрических слипаний, точное значение функции Шеннона длины диагностического теста относительно множественных монотонных симметри-

ческих слипаний, высокая нижняя оценка функции Шеннона длины диагностического теста относительно единичных дизъюнктивных слипаний.

2.2 Проверяющий тест относительно множественных монотонных симметрических слипаний переменных

Будем говорить, что набор $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ больше набора $\tilde{\beta} = (\beta_1, \dots, \beta_n)$, если $\alpha_i \geq \beta_i$ и $\tilde{\alpha} \neq \tilde{\beta}$. Будем обозначать данное отношение как $\tilde{\alpha} \prec \tilde{\beta}$.

Определение 3. Порогом монотонной или антимонотонной симметрической функции будем называть такое число k , что значения функции на k -м и $(k + 1)$ -м слоях булева куба различаются.

В данной главе удобно переопределить понятие проверяющей пары, добавив еще одно условие к определению из предыдущей главы.

Определение 4. Проверяющей парой для переменных $x_i, x_j, i \neq j$, назовем пару наборов $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n), \tilde{\beta} = (\beta_1, \dots, \beta_n)$, обладающих следующими свойствами:

- $f(\alpha_1, \dots, \alpha_n) \neq f(\beta_1, \dots, \beta_n)$,
- $\alpha_k \neq \beta_k$ при $k \in \{i, j\}$,
- $\alpha_i \oplus \alpha_j = \beta_i \oplus \beta_j = 1$,
- $\alpha_k = \beta_k$ в остальных случаях.

Определение 5. Проверяющей тройкой для переменных x_i, x_j назовем такие наборы $\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3$, что:

- $f(\tilde{\alpha}_1) = f(\tilde{\alpha}_3) \neq f(\tilde{\alpha}_2)$,
- в позициях i, j набора $\tilde{\alpha}_1$ стоят нули,

- набор $\tilde{\alpha}_2$ является соседним с $\tilde{\alpha}_1$ по одной из компонент i или j , а набор $\tilde{\alpha}_3$ соседний с $\tilde{\alpha}_2$ по другой компоненте.

Определение 6. Проверяющей четверкой для переменных x_i, x_j назовем наборы $\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3, \tilde{\alpha}_4$, такие, что:

- $f(\tilde{\alpha}_1) \neq f(\tilde{\alpha}_2), f(\tilde{\alpha}_3) \neq f(\tilde{\alpha}_4)$,
- у набора $\tilde{\alpha}_1$ стоят нули в разрядах i, j , а у $\tilde{\alpha}_3$ стоит ноль в одном из разрядов i, j (обозначим этот разряд через t) и единица в другом разряде,
- наборы $\tilde{\alpha}_1$ и $\tilde{\alpha}_2$ являются соседними по компоненте t , наборы $\tilde{\alpha}_3$ и $\tilde{\alpha}_4$ также являются соседними по компоненте t ,
- $\tilde{\alpha}_1 \prec \tilde{\alpha}_2 \prec \tilde{\alpha}_4, \tilde{\alpha}_1 \prec \tilde{\alpha}_3 \prec \tilde{\alpha}_4$.

Определение 7. Множество наборов называется дизъюнктивным (конъюнктивным) детектором, если для каждой пары переменных x_i, x_j в нем есть два набора $\tilde{\alpha}_1, \tilde{\alpha}_2$, такие, что:

- наборы $\tilde{\alpha}_1, \tilde{\alpha}_2$ являются соседними по одной из компонент i, j , причем у набора $\tilde{\alpha}_2$ ($\tilde{\alpha}_1$) в позициях i и j стоят единицы (нули),
- $f(\tilde{\alpha}_1) \neq f(\tilde{\alpha}_2)$,
- $\forall \tilde{\alpha} : \tilde{\alpha}_2 \prec \tilde{\alpha} \Rightarrow f(\tilde{\alpha}_2) = f(\tilde{\alpha})$ ($\forall \tilde{\alpha} : \tilde{\alpha} \prec \tilde{\alpha}_1 \Rightarrow f(\tilde{\alpha}_1) = f(\tilde{\alpha})$). (Выбранные два набора обнаруживают дизъюнктивные (конъюнктивные) слияния переменных x_i, x_j).

Определение 8. Пусть $h(x_1, \dots, x_s)$ — монотонная или антимонотонная симметрическая функция. Множество наборов $\tilde{\alpha}_0, \tilde{\alpha}_1, \dots, \tilde{\alpha}_s$ называется x_i -детектором, если выполнено следующее:

- наборы $\tilde{\alpha}_0$ и $\tilde{\alpha}_i$ являются соседними по i -й компоненте, причем $\tilde{\alpha}_0 \prec \tilde{\alpha}_i$,

- $h(\tilde{\alpha}_0) \neq h(\tilde{\alpha}_i)$,
- при $j \in \{1, \dots, i-2, i-1, i+1, i+2, \dots, s\}$ и нулевой j -й компоненте набора $\tilde{\alpha}_0$ набор $\tilde{\alpha}_j$ является соседним с $\tilde{\alpha}_0$ по j -й компоненте, а при единичной — соседним с $\tilde{\alpha}_i$ по j -й компоненте.

Назовем $\tilde{\alpha}_0$ *нижним ведущим набором* x_i -детектора, а $\tilde{\alpha}_i$ — *верхним ведущим набором* x_i -детектора.

Далее докажем ряд вспомогательных лемм. При их доказательстве под $(s+1)$ -й компонентой s -мерного вектора будем понимать 1-ю компоненту, под $(s+2)$ -й — 2-ю и так далее. То есть, для удобства считаем сложение „циклическим“, когда говорим о номерах разрядов в булевых наборах.

Лемма 11. Пусть $1 \leq k \leq s$, $h(y_1, \dots, y_s)$ — симметрическая функция, которая на k -м слое куба равна a , на всех остальных слоях — $\bar{a}$. Тогда существует множество наборов, содержащее хотя бы по одной проверяющей тройке для каждой пары переменных, мощности не более, чем $\frac{s^2}{2} + D_1 s$, где D_1 — некоторая вещественная константа.

Доказательство. Будем последовательно отбирать проверяющие тройки для пар переменных $(y_1, y_2), (y_1, y_3), \dots, (y_1, y_s), \dots, (y_{s-1}, y_s)$.

Пусть $k \leq \frac{s}{2}$. Для всех $i \in \{1, \dots, n-1\}$ оценим число наборов, содержащих проверяющие тройки для $(y_i, y_{i+1}), \dots, (y_i, y_s)$. Возьмем некоторый набор $\tilde{\alpha}_1^i$, в котором на позициях $i, i+1, \dots, (i+s-k)$ стоят нули, а на остальных — единицы, и набор $\tilde{\alpha}_2^i$, соседний с $\tilde{\alpha}_1^i$ по i -й компоненте. Теперь возьмем наборы, соседние с $\tilde{\alpha}_2^i$ по компонентам $i+1, \dots, \min(s, i+s-k)$. Среди выбранных наборов содержатся проверяющие тройки для $(y_i, y_{i+1}), \dots, (y_i, y_{\min(s, i+s-k)})$. Если $i+s-k < s$, то возьмем набор $\tilde{\beta}_1^i$, в котором на позициях $i, i+s-k+1, i+s-k+2, \dots, i+2(s-k)$ стоят нули, а на остальных — единицы, и набор $\tilde{\beta}_2^i$, соседний с $\tilde{\beta}_1^i$ по i -й компоненте. И также возьмем наборы, соседние с $\tilde{\beta}_2^i$ по компонентам $i+s-k+1, \dots, s$.

Всего для данного i выбрано наборов не более, чем $s - i + 4$. Тогда существует такая константа D_1 , что суммарно для всех переменных выбрано наборов не более, чем $\frac{s^2}{2} + D_1 s$. Для каждой пары переменных среди выбранных наборов есть проверяющая тройка.

Пусть теперь $k > \frac{s}{2}$. Заметим, что в предыдущем варианте мы выбирали проверяющие тройки так, что первые два набора были общими у некоторых троек. В текущем случае будем выбирать наборы аналогично, только общими у проверяющих троек будут последние два набора. Получаем ту же верхнюю оценку $\frac{s^2}{2} + D_1 s$ для множества наборов, содержащего проверяющие тройки для всех пар переменных.

□

Лемма 12. Пусть $h(y_1, \dots, y_s)$ — симметрическая функция и существуют числа $k_0, k_1, k_0 < k_1$, такие, что функция $h(y_1, \dots, y_s)$ принимает значение a на слоях $0, 1, \dots, k_0 - 1$, значение $\bar{a}$ на слое k_0 , значение b на слое k_1 и значение $\bar{b}$ на слоях $k_1 + 1, \dots, s$. Тогда существует множество наборов, содержащее хотя бы по одной проверяющей четверке для каждой пары переменных, мощности $\frac{s^2}{2} + D_2 s$, где D_2 — некоторая вещественная константа.

Доказательство. Будем последовательно добавлять проверяющие четверки для переменных $(y_1, y_2), (y_1, y_3), \dots, (y_1, y_s), \dots, (y_{s-1}, y_s)$.

Пусть $k_0 < \frac{s}{2}$. Получим оценку числа наборов, содержащих проверяющие четверки для $(y_i, y_{i+1}), \dots, (y_i, y_s)$. Возьмем набор $\tilde{\alpha}_1^i$, у которого на позициях $i, i + 1, \dots, i + s - k_0$ стоят нули, а на остальных — единицы. Возьмем набор $\tilde{\alpha}_2^i$, соседний с $\tilde{\alpha}_1^i$ по i -й компоненте. Это будут первые два набора проверяющих четверок. Далее будем последовательно получать вторые два набора проверяющих четверок следующим образом. Получим два новых набора, заменив нулевые компоненты $i + 1, \dots, i + k_1 - k_0 + 1$ наборов $\tilde{\alpha}_1^i, \tilde{\alpha}_2^i$ единицами. Построенные четыре набора являются проверяющими четверками для пар переменных

$(y_i, y_{i+1}), (y_i, y_{i+2}), \dots, (y_i, y_{i+k_1-k_0+1})$. Затем заменим следующие $k_1 - k_0 + 1$ нулевые компоненты $\tilde{\alpha}_1^i, \tilde{\alpha}_2^i$ единицами и получим еще два набора. Когда более не будет следующих $k_1 - k_0 + 1$ компонент, процесс прекращается. Если при этом остались ни разу не инвертированные нулевые компоненты в позициях с номерами больше i , получим еще два набора, заменив разряды $i + s - k_0 - (k_1 - k_0), \dots, i + s - k_0 + 1$ единицами. Затем, если $i + s - k_0 < s$, возьмем набор $\tilde{\beta}_1^i$, у которого нули в компонентах $i, i + s - k_0 + 1, \dots, i + 2(s - k_0 + 1)$, и $\tilde{\beta}_2^i$, соседний с $\tilde{\beta}_1^i$ по i -й компоненте. Аналогичным образом будем добавлять единицы к наборам $\tilde{\beta}_1^i, \tilde{\beta}_2^i$ группами по $k_1 - k_0 + 1$ единиц, начиная с $(s - k_0 + 1)$ -й компоненты, пока не будут получены наборы с единицами в s -й компоненте.

Оценим сверху число добавленных наборов. Для переменной y_i было добавлено не более, чем $2 \cdot \frac{s - i}{k_1 - k_0 + 1} + 2 + 2 + 4$ наборов. Тогда существует константа D_2 , что для всех переменных добавлено не более, чем $\frac{s^2}{k_1 - k_0 + 1} + D_2 s \leq \frac{s^2}{2} + D_2 s$ наборов. В выбранном множестве есть проверяющие четверки для всех пар переменных.

Пусть $k_0 \geq \frac{s}{2}$. Но тогда $k_1 > \frac{s}{2}$. Тогда множество наборов строится аналогично, только общими у проверяющих четверок будут не первые, а вторые два набора. Получаем аналогичную оценку множества, содержащего проверяющие четверки для всех пар переменных.

□

Лемма 13. Пусть $h(y_1, \dots, y_s)$ — отличная от константы монотонная или антимонотонная симметрическая функция с порогом k . Тогда существует дизъюнктивный детектор $T_\vee$ мощности $|T_\vee| \leq \frac{s^2}{2k} + D_3 s \log s$, и конъюнктивный детектор $T_\&$ мощности $|T_\&| \leq \frac{s^2}{2(s - k)} + D_4 s \log s$, где D_3 и D_4 — некоторые вещественные константы.

Доказательство. Пусть $k \leq \frac{s}{2}$. Обозначим $t = \left\lceil \frac{s}{k} \right\rceil$. Возьмем t наборов $\tilde{\alpha}_1, \dots, \tilde{\alpha}_t$, таких, что при $i \in \{1, \dots, t\}$ в компонентах с номерами $(i-1)k+1, \dots, ik$ набора $\tilde{\alpha}_i$ стоят единицы, а в остальных — нули. Выбранные наборы назовем *основными* наборами.

Далее добавим *дополнительные* наборы. Дополнительный набор определяется натуральным числом p и целыми неотрицательными числами $r, l_1, \dots, l_{2^r}$, такими, что $\sum_{j=1}^{2^r} l_j - (p-1) \leq n$, следующим способом. Первые l_1 разрядов набора, начиная с p -го, равны 1, следующие $l_2 - 0$, следующие $l_3 - 1$ и так далее. Эти $l_1 + l_2 + \dots + l_{2^r}$ разрядов назовем *рабочими*. Все остальные разряды дополнительного набора положим равными нулю. Число p в данном определении назовем *начальной позицией*, 2^r — *числом длин*, а $l_1, \dots, l_{2^r}$ — *последовательностью длин*.

Опишем процесс добавления дополнительных наборов.

Последовательно перебираются возможные начальные позиции из множества $\left\{1, 2k+1, \dots, \left(\left\lceil \frac{s}{2k} \right\rceil - 1\right)2k+1\right\}$.

Пусть текущая начальная позиция равна p' . В первом дополнительном наборе в позициях $p', \dots, p'+k-1$ стоят единицы, в остальных — нули. Этот набор задается указанной начальной позицией, числом длин 2, последовательностью длин k, k (это не единственный способ задать данный набор, но мы будем пользоваться именно таким способом). Заметим, что этот набор уже содержится среди основных. Пусть $\tilde{\gamma}$ — последний добавленный набор с начальной позицией p' . Он задается начальной позицией p' , числом длин $2^{r'}$, последовательностью длин $l_1, \dots, l_{2^{r'}}$. Определим последовательность чисел $m_1, \dots, m_{2^{r'}+1}$ следующим образом. Последовательно перебираем значения i из множества $\{1, 3, 5, \dots, 2^{r'}-1\}$.

Если $l_i \leq 1, l_{i+1} \leq 1$, то $m_{2i-1} = l_i, m_{2i} = l_{i+1}, m_{2i+1} = 0, m_{2i+2} = 0$.

Если $l_i = l_{i+1} = 2t$, то $m_{2i-1} = t, m_{2i} = t, m_{2i+1} = t, m_{2i+2} = t$.

Если $l_i = l_{i+1} = 2t+1$, то $m_{2i-1} = t+1, m_{2i} = t, m_{2i+1} = t, m_{2i+2} = t$.

Если $l_i = 2t + 1$, $l_{i+1} = 2t$, то $m_{2i-1} = t + 1$, $m_{2i} = t$, $m_{2i+1} = t$, $m_{2i+2} = t$.

Если $l_i = 2t + 2$, $l_{i+1} = 2t + 1$, то $m_{2i-1} = t + 1$, $m_{2i} = t + 1$, $m_{2i+1} = t + 1$, $m_{2i+2} = t$.

Если $l_i = 2t$, $l_{i+1} = 2t + 1$, то $m_{2i-1} = t$, $m_{2i} = t$, $m_{2i+1} = t$, $m_{2i+2} = t + 1$.

Если $l_i = 2t + 1$, $l_{i+2} = 2t + 2$, то $m_{2i-1} = t$, $m_{2i} = t + 1$, $m_{2i+1} = t + 1$, $m_{2i+2} = t + 1$.

Определим набор $\tilde{\gamma}'$ с числом длин $2^{r'+1}$, последовательностью длин $m_1, \dots, m_{2^{r'+1}}$ и начальной позицией p' . Если $\tilde{\gamma} \neq \tilde{\gamma}'$, добавляем его к множеству дополнительных наборов, в противном случае переходим к следующей начальной позиции. Процесс завершается, когда перебраны все начальные позиции.

Приведем пример дополнительных наборов для $n = 12, k = 5$:

$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$, $(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$,
 $(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$, $(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$,
 $(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$, $(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$,
 $(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$, $(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$.

Заметим, что для любой пары переменных x_i, x_j в множестве основных и дополнительных наборов есть хотя бы один набор k -го слоя, в котором i -я и j компоненты не равны друг другу.

Число дополнительных наборов не более, чем $\left\lceil \frac{s}{2k} \right\rceil \lceil \log k \rceil$. Теперь к каждому дополнительному набору добавим все наборы, соседние с ним по нулевым рабочим разрядам. Таких наборов ровно k для каждого дополнительного набора. Заметим, что для любых пар i, j , таких, что при некотором q , $2kq < i < j \leq 2k(q + 1)$, существует пара наборов, обнаруживающих дизъюнктивное слипание x_i, x_j . Всего дополнительных наборов вместе с их соседними не более, чем $(k + 1) \left\lceil \frac{s}{2k} \right\rceil \lceil \log k \rceil \leq s \log s + D'_3 s$, где D'_3 — некоторая вещественная константа.

Затем к первому основному добавим все наборы, соседние с ним по компонентам $k + 1, \dots, s$. К i -му основному набору добавим все наборы, соседние с ним по компонентам $ik + 1, \dots, s$. Итого, на данном шаге добавлено наборов $s - k + s - 2k + \dots + s - (\lceil \frac{s}{k} \rceil - 1)k \leq \frac{s}{2} \lfloor \frac{s}{k} \rfloor$. Теперь для всех пар переменных найдены пары наборов, обнаруживающие дизъюнктивные слипания этих переменных. Подсчитывая общее число найденных наборов, получаем, что существует вещественная константа D_3 , при которой выполняется верхняя оценка, требуемая в лемме.

Поменяв местами 0 и 1, k и $s - k$, аналогичным образом строим конъюнктивный детектор мощности не более, чем $\frac{s}{2} \lfloor \frac{s}{s - k} \rfloor + D_4 s \log s$, где D_4 — некоторая вещественная константа.

Если $k > \frac{s}{2}$, то проводим доказательство аналогично, поменяв местами нули и единицы.

□

Лемма 14. Пусть $h(y_1, \dots, y_s)$ — монотонная или антимонотонная симметрическая функция с порогом k . Тогда существует множество наборов T , которое содержит y_1 -детектор, ..., y_s -детектор, причем $|T| \leq s \min(k, s - k) + D_5 s$.

Доказательство. Пусть $k \leq \frac{s}{2}$. Возьмем набор $\tilde{\beta}$, в котором первые $s - k$ компонент равны нулю, остальные — единице. Возьмем наборы $\tilde{\beta}_1, \dots, \tilde{\beta}_{s-k}$, которые являются соседними с $\tilde{\beta}$ по компонентам $1, \dots, s - k$ соответственно. Для каждого из наборов $\tilde{\beta}_i$ возьмем k наборов $\tilde{\beta}_i^{s-k+1}, \dots, \tilde{\beta}_i^s$, которые являются соседними с $\tilde{\beta}_i$ по компонентам $s - k + 1, \dots, s$ соответственно. Заметим, что среди выбранных наборов содержатся $y_1, \dots, y_{s-k}$ -детекторы. Всего выбрано $s - k + 1 + k(s - k)$ наборов.

Затем возьмем набор $\tilde{\gamma}$, в котором последние $(s - k)$ компонент равны нулю, а остальные — единице. Возьмем наборы $\tilde{\gamma}_{k+1}, \dots, \tilde{\gamma}_s$, которые являются соседними с $\tilde{\gamma}$ по компонентам $k + 1, \dots, s$ соответственно. При $j \geq s - k + 1$ для каждого

из наборов $\tilde{\gamma}_j$ возьмем k наборов $\tilde{\gamma}_j^1, \dots, \tilde{\gamma}_j^k$, которые являются соседними с $\tilde{\gamma}_j$ по компонентам $1, \dots, k$ соответственно. Среди выбранных наборов содержатся $y_{s-k+1}, \dots, y_s$ -детекторы. В этом случае всего выбрано $s - k + 1 + k^2$ наборов.

Теперь, объединив выбранные наборы, получаем искомое множество мощности $2(s - k + 1) + sk$ наборов. Если же $k > \frac{s}{2}$, то, поменяв местами нули и единицы и k и $s - k$ в доказательстве предыдущего случая, получим искомое множество мощности $2(k + 1) + (s - k)k$.

Нетрудно выбрать константу D_5 , что выполнялась верхняя оценка, указанная в лемме. □

Теперь перейдем к доказательству теоремы.

Теорема 8 [14]. *При $n \rightarrow \infty$ имеет место неравенство:*

$$2n \leq L_{\text{detect}}(n, MQ(\Phi_{\text{ms}})) \leq \frac{n^2}{2} + O(n \log n).$$

Доказательство. Докажем нижнюю оценку. Рассмотрим функцию $f(x_1, \dots, x_n) = x_1 x_2 \dots x_n \vee \bar{x}_1 \dots \bar{x}_n$. Эта же функция была использована в [6] при изучении тестов для некоторого подмножества неисправностей, рассматриваемых в данной работе. Пусть в тест не входят 2 набора $(n - 1)$ -го слоя куба. В одном наборе ноль стоит в позиции i , в другом — в позиции j . Тогда дизъюнктивное слипание этих двух переменных не будет проверено. Аналогично, если некоторые 2 набора первого слоя куба отсутствуют в тесте, не будет проверено конъюнктивное слипание некоторых двух переменных. Пусть в тест не входит нулевой набор. Тогда неисправность, связанная с подстановкой единицы вместо x_i , может быть проверена только на наборе $(n - 1)$ -го слоя, в котором i -й разряд равен нулю. Поэтому либо в тест входит нулевой набор, либо все наборы $(n - 1)$ -слоя. Используя подстановку нуля, аналогично доказываем, что в тест входят либо все наборы 1-го слоя, либо единичный набор.

Докажем верхнюю оценку. Пусть $f(x_1, \dots, x_n)$ — исходная функция. Сначала заметим, что если хоть одна существенная переменная участвует в констант-

ном слипании, неисправность обнаруживается на тесте существенности. Поэтому для проверки наличия константных слипаний достаточно не более, чем $2n$ наборов. Далее будем рассматривать только неконстантные слипания.

Воспользуемся результатами, полученными в [40, 50]. В этих работах исследовались тесты относительно перестановок переменных. В булевой функции $f(x_1, \dots, x_n)$ произошла транспозиция переменных $x_i, x_j, i < j$, если вместо исходной булевой функции реализуется функция неисправности $g(x_1, \dots, x_n) = f(x_1, \dots, x_{i-1}, x_j, x_{i+1}, \dots, x_{j-1}, x_i, x_{j+1}, \dots, x_n)$. Если $\exists \tilde{\alpha} : f(\tilde{\alpha}) \neq g(\tilde{\alpha})$, то транспозиция переменных x_i, x_j обнаруживается, в противном случае — необнаруживается. В [40] введено бинарное отношение R_f на множестве переменных $x_1, \dots, x_n$ следующим образом: $x_i R_f x_j \iff$ транспозиция переменных x_i, x_j необнаруживается. Доказано, что R_f — отношение эквивалентности.

Введем бинарное отношение Q_f на множестве переменных функции $f(\tilde{x}^n)$ следующим образом. Всегда верно, что $x_i Q_f x_i$. Если $i \neq j$, то $x_i Q_f x_j$ тогда и только тогда, когда для переменных x_i, x_j функции $f(\tilde{x}^n)$ не существует проверяющей пары. Очевидно, что $x_i R_f x_j \iff x_i Q_f x_j$, следовательно, Q_f — отношение эквивалентности и переменные $x_1, \dots, x_n$ разбиваются на непересекающиеся классы эквивалентности по отношению Q_f . Каждый класс будем называть *множеством симметричности*.

Без ограничения общности будем считать, что переменные $x_1, \dots, x_{m_1}$ образуют первое множество симметричности, $x_{m_1+1}, \dots, x_{m_2}$ — второе множество симметричности, ..., $x_{m_{r-1}+1}, \dots, x_{m_r}$ — r -е множество симметричности, а, начиная с x_{m_r+1} , каждая переменная образует отдельное множество симметричности.

Если переменные x_i, x_j из разных множеств симметричности участвуют в одном слипании, то для обнаружения данной неисправности достаточно проверяющей пары для данных переменных. Построим множество, содержащее проверяющие пары для всевозможных пар переменных из разных множеств сим-

метричности. В работе [50] был построен проверяющий тест T_{permut} мощности $\Theta(n \log n)$ относительно всевозможных перестановок переменных. Частным случаем перестановки является единичная транспозиция переменных, определенная выше. Легко видеть, что транспозицию переменных x_i, x_j можно обнаружить на наборе $\tilde{\alpha}$ тогда и только тогда, когда существует набор $\tilde{\beta}$ такой, что $\tilde{\alpha}, \tilde{\beta}$ — проверяющая пара для переменных x_i, x_j . Следовательно, к T_{permut} достаточно добавить не более одного набора, чтобы в нем содержалась проверяющая пара для x_i, x_j . Всего число пар переменных, для которых есть проверяющая пара, равно $C_n^2 - C_{m_1}^2 - C_{m_2-m_1}^2 - \dots - C_{m_r-m_{r-1}}^2$. Следовательно, существует множество T_{detect} , содержащее хотя бы по одной проверяющей паре для всевозможных пар переменных из разных множеств симметричности, причем $|T_{\text{detect}}| \leq C_n^2 - \sum_{i=0}^r C_{m_{i+1}-m_i}^2 + O(n \log n)$, где m_0 полагаем равным 0.

Множество T_{detect} обнаруживает все множественные слипания, при которых хотя бы в одном слипании участвуют переменные разных множеств симметричности. Рассмотрим оставшиеся неисправности. Далее будем последовательно добавлять к T_{detect} наборы, обнаруживающие слипания внутри очередного множества симметричности. Опишем процесс на примере первого множества симметричности.

Случай 0. Переменные $x_1, \dots, x_{m_1}$ фиктивны. Их слипания не меняют исходную функцию, переходим к следующему множеству симметричности.

Случай 1. Существуют такие числа $a_{m_1+1}, \dots, a_n$, при которых функция $h(x_1, \dots, x_{m_1}) = f(x_1, \dots, x_{m_1}, a_{m_1+1}, \dots, a_n)$ не является ни монотонной, ни антимонотонной.

Подслучай 1а. Функция $h(x_1, \dots, x_{m_1})$ на k -м слое куба равна a , на всех остальных слоях — $\bar{a}$. Заметим, что k не может равняться 0 или n , так как функция будет монотонной или антимонотонной.

По лемме 11 можно построить множество, содержащее все проверяющие тройки для любых пар переменных из $x_1, \dots, x_{m_1}$ мощности не более, чем $\frac{m_1^2}{2} + D_1 m_1$. Приписав к каждому набору числа $a_{m_1+1}, \dots, a_n$, получим множество T_1 той же мощности, содержащее проверяющие тройки для переменных $x_1, \dots, x_{m_1}$ функции $f(x_1, \dots, x_n)$. Выберем проверяющую тройку $\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3$ для произвольных переменных x_i, x_j из первого множества симметричности. У исправной функции значение на наборе $\tilde{\alpha}_2$ должно отличаться от значений на наборах $\tilde{\alpha}_1$ и $\tilde{\alpha}_3$. Если же переменные x_i и x_j участвуют в одном слипании, то либо на $\tilde{\alpha}_1, \tilde{\alpha}_2$, либо на $\tilde{\alpha}_2, \tilde{\alpha}_3$ значения функции неисправности будут совпадать. Построенное множество обнаруживает всевозможные неисправности, при которых в одном слипании участвуют переменные из первого множества симметричности.

Подслучай 1b. Существуют числа $k_0, k_1, k_0 < k_1$, такие, что функция $h(y_1, \dots, y_{m_1})$ принимает значение a на слоях $0, 1, \dots, k_0 - 1$, значение $\bar{a}$ на слое k_0 , значение b на слое k_1 и значение $\bar{b}$ на слоях $k_1 + 1, \dots, n$.

По лемме 12 можно построить множество, содержащее все проверяющие четверки для любых пар переменных из $x_1, \dots, x_{m_1}$ мощности не более, чем $\frac{m_1^2}{2} + D_2 m_1$. Приписав справа к каждому набору числа $a_{m_1}, \dots, a_n$ получим множество T_2 той же мощности, содержащее проверяющие четверки для переменных $x_1, \dots, x_{m_1}$ функции $f(x_1, \dots, x_n)$.

Если произошло слипание, в котором участвуют переменные x_i, x_j первого множества симметричности, то либо на первых двух, либо на последних двух наборах проверяющей четверки функция неисправности будет принимать одинаковые значения, поэтому неисправность будет обнаружена. Построенное множество обнаруживает всевозможные неисправности при которых в одном слипании участвуют переменные из первого множества симметричности.

Случай 2. При любых $b_{m_1+1}, \dots, b_n$ функция $f(x_1, \dots, x_{m_1}, b_{m_1+1}, \dots, b_n)$ будет монотонной или антимонотонной симметрической функцией. Выберем числа $a_{m_1+1}, \dots, a_n$ так, что функция $h(x_1, \dots, x_{m_1}) = f(x_1, \dots, x_{m_1}, a_{m_1+1}, \dots, a_n)$ имеет максимально возможный порог k .

По лемме 13 построим множества $T'_\vee$ и $T'_\&$, являющиеся дизъюнктивным и конъюнктивным детекторами для функции $h(x_1, \dots, x_{m_1})$. К каждому набору этих множеств припишем справа числа $a_{m_1}, \dots, a_n$, получим множества $T_\vee$ и $T_\&$. В исправной функции на двух наборах, проверяющих дизъюнктивные слипания любой пары переменных из первого множества симметричности, должны реализовываться разные значения. Если же эти переменные участвуют в одном дизъюнктивном слипании, то значения будут одинаковыми. Аналогично с конъюнктивными слипаниями. В множествах $T_\vee$ и $T_\&$ для каждой пары переменных есть наборы, проверяющие их дизъюнктивное и конъюнктивное слипания. Поэтому далее можно считать, что нет дизъюнктивных и конъюнктивных слипаний переменных среди первого множества симметричности.

Далее, для $h(x_1, \dots, x_{m_1})$ по лемме 14 построим множество, являющееся x_1 -детектором, ..., x_{m_1} -детектором. Покажем, что x_j -детектор (обозначим T_{x_j}) обнаруживает все неисправности, при которых x_j участвует в каком-либо слипании, кроме, быть может, слипания переменных $x_1, \dots, x_{m_1}$. Пусть x_j -детектор $T_{x_j} = \{\tilde{\alpha}_0^j, \tilde{\alpha}_1^j, \dots, \tilde{\alpha}_{m_1}^j\}$, где $\tilde{\alpha}_0^j, \tilde{\alpha}_j^j$ — верхний и нижний ведущие наборы.

Пусть $f'(x_1, \dots, x_n)$ — функция неисправности, получающаяся из $f(x_1, \dots, x_n)$ в результате множественного слипания. Через $|\tilde{\alpha}|_{d_1, \dots, d_q}$ обозначим число единиц набора $\tilde{\alpha}$ в позициях $d_1, \dots, d_q$, через $\tilde{\alpha}(d)$ — значение d -го разряда набора $\tilde{\alpha}$.

Определим наборы $\tilde{\beta}_0^j, \tilde{\beta}_1^j, \dots, \tilde{\beta}_{m_1}^j$ следующим образом. Если переменная x_r не участвует в слипаниях, то $\tilde{\beta}_i^j(r) = \tilde{\alpha}_i^j(r)$. Если переменная x_r участвует в некотором слипании, для которого функция слипания есть $\varphi(x_{d_1}, \dots, x_{d_q})$, то $\tilde{\beta}_i^j(r) = \varphi(\tilde{\alpha}_i^j(d_1), \dots, \tilde{\alpha}_i^j(d_q))$. Ясно, что $f(\tilde{\beta}_i^j) = f'(\tilde{\alpha}_i^j)$.

Пусть также произошло слипание переменных $x_{l_{p+1}}, \dots, x_{l_s}$ из первого множества симметричности, а функция данного слипания $\varphi_2(x_{l_{p+1}}, \dots, x_{l_s})$. Если на их местах стоят нули в ведущих наборах, то $f'(\tilde{\alpha}_{l_{p+1}}^j) = f'(\tilde{\alpha}_0^j)$, поскольку слипание не является дизъюнктивным и $f(\tilde{\alpha}_{l_{p+1}}^j) \neq f(\tilde{\alpha}_0^j)$. Неисправность обнаружена. Аналогично неисправность будет обнаружена в случае единиц, так как слипание не конъюнктивное.

Далее будем считать, что $\tilde{\alpha}_0^j(l_{p+1}) = 0$, $\tilde{\alpha}_0^j(l_{p+2}) = 1$. Возьмем из T_j набор $\tilde{\alpha}_{l_{p+1}}^j$. Если $f'(\tilde{\alpha}_0^j) = f'(\tilde{\alpha}_{l_{p+1}}^j)$, то неисправность обнаружена, так как $f(\tilde{\alpha}_0^j) = f(\tilde{\alpha}_{l_{p+1}}^j)$. В противном случае порог функции $\varphi_2(x_{l_{p+1}}, \dots, x_{l_s})$ равен $|\tilde{\alpha}_0^j|_{l_{p+1}, \dots, l_s}$. Поскольку $|\tilde{\alpha}_{l_{p+2}}^j|_{l_{p+1}, \dots, l_s} < |\tilde{\alpha}_j^j|_{l_{p+1}, \dots, l_s} = |\tilde{\alpha}_0^j|_{l_{p+1}, \dots, l_s}$, получаем $\tilde{\beta}_{l_{p+2}}^j = \tilde{\beta}_j^j$, $f(\tilde{\beta}_{l_{p+2}}^j) = f(\tilde{\beta}_j^j)$, $f'(\tilde{\alpha}_{l_{p+2}}^j) = f'(\tilde{\alpha}_j^j)$. Неисправность обнаружена, так как $f(\tilde{\alpha}_{l_{p+2}}^j) \neq f(\tilde{\alpha}_j^j)$.

Теперь пусть нет слипаний без участия x_j , но есть хотя бы одна переменная x_q , не участвующая в слипаниях. Допустим, $\tilde{\alpha}_0^j(q) = \tilde{\alpha}_j^j(q) = 0$. Заметим, что в слипании с x_j участвует хотя бы одна переменная x_t , равная единице в ведущих наборах, иначе порог функции $\varphi_1(x_{l_1}, \dots, x_{l_p})$ был бы равен p и слипание было бы конъюнктивным. Поэтому $\tilde{\beta}_0^j(t) = 0$. Других слипаний в первом множестве симметричности не было, поэтому $|\tilde{\beta}_0^j|_{1, \dots, m_1} < k$, $|\tilde{\beta}_t^j|_{1, \dots, m_1} < k + 1$, поэтому $f(\tilde{\beta}_0^j) = f(\tilde{\beta}_t^j)$, $f'(\tilde{\alpha}_0^j) = f'(\tilde{\alpha}_t^j)$ и неисправность обнаружена. Случай, когда $\tilde{\alpha}_0^j(q) = \tilde{\alpha}_j^j(q) = 1$, доказывается аналогично.

Непроверенной остается неисправность, при которой все переменные множества симметричности составляют одно слипание. Заметим, что порогом функции слипания может быть только число k , иначе на всех поданных наборах функция принимала бы одно значение.

Если при всех значениях переменных вне первого множества симметричности реализуется либо константная функция, либо монотонная или антимонотонная симметрическая функция с порогом k , тогда указанное выше слипание

не меняет реализуемую функцию. В противном случае зафиксируем остальные переменные так, чтобы реализовывалась некоторая монотонная или антимонотонная симметрическая функция $h'(x_1, \dots, x_{m_1})$ с порогом k' , $k' < k$. Возьмем любые два набора k' -го и $(k' + 1)$ -го слоев булева куба. На них исходная функция должна принимать разные значения, а в случае слипания всех переменных с порогом k — одинаковые. Добавим в тест два n -мерных набора, соответствующих выбранным m_1 -мерным наборам. Теперь проверены всевозможные слипания, в которых участвуют переменные первого множества симметричности. Для этого потребовалось не более, чем $\frac{m_1^2}{2k} + \frac{m_1^2}{2(m_1 - k)} + m_1 \min(k, m_1 - k) + D_6 m_1 \log m_1 \leq \frac{m_1^2}{2} + D_7 m_1 \log m_1$, где D_6 и D_7 — некоторые вещественные константы.

Объединив все случаи, получаем, что существует такая вещественная константа D , что для первого множества симметричности в тест было добавлено не более, чем $\frac{m_1^2}{2} + D m_1 \log m_1$ наборов.

Аналогично разбираем остальные множества симметричности. Получим, что для i -го множества симметричности в тест добавлено не более, чем $\frac{(m_i - m_{i-1})^2}{2} + D(m_i - m_{i-1}) \log(m_i - m_{i-1})$ наборов (напомним, что m_0 считается равным нулю). Теперь оценим мощность построенного теста: $|T_{\text{detect}}| + \sum_{i=1}^r \left(\frac{(m_i - m_{i-1})^2}{2} + D(m_i - m_{i-1}) \log(m_i - m_{i-1}) \right) \leq C_n^2 - \sum_{i=1}^r C_{m_{i+1}-m_i}^2 + O(n \log n) + \sum_{i=1}^r \left(\frac{(m_i - m_{i-1})^2}{2} + D(m_i - m_{i-1}) \log(m_i - m_{i-1}) \right) \leq \frac{n^2}{2} + O(n \log n)$. Последнее неравенство получается из того, что $\log(m_i - m_{i-1}) \leq \log n$, а $\sum_{i=0}^r D(m_i - m_{i-1}) = O(n)$.

□

2.3 Диагностический тест относительно монотонных симметрических слипаний переменных

Теорема 9 [14]. *Имеет место равенство: $L_{\text{diagn}}(n, MQ(\Phi_{\text{ms}})) = 2^n$.*

Доказательство. Вновь обозначим через $f_{x_{i_1}, \dots, x_{i_k}}^{\varphi(x_{i_1}, \dots, x_{i_k})}(x_1, \dots, x_n)$ функцию, получающуюся из $f(x_1, \dots, x_n)$ в результате слипания переменных $x_{i_1}, \dots, x_{i_k}$, когда функция слипания равна $\varphi(x_{i_1}, \dots, x_{i_k})$.

Рассмотрим функцию $f(x_1, \dots, x_n) = x_1 \dots x_n$. Предположим, что некоторый набор $\tilde{\alpha}$ не входит в тест. Пусть его компоненты с номерами $j_1, \dots, j_s$ равны нулю, а остальные — единице. Но тогда функции неисправности $f_{x_{j_1}, \dots, x_{j_s}}^{x_{j_1} \vee \dots \vee x_{j_s}}(x_1, \dots, x_n)$ и $f_{x_{j_1}, \dots, x_{j_s}}^1(x_1, \dots, x_n)$ не будут различаться тестом. Поэтому в диагностический тест для конъюнкции должны войти все наборы.

□

Данная теорема также справедлива для $Q(\Phi_{\text{ms}})$.

2.4 Диагностический тест относительно дизъюнктивных слипаний переменных

В данной части будет доказана теорема, из которой следует, что функция Шеннона длины диагностического теста относительно дизъюнктивных слипаний равна $2^{n-O(\log n)}$

Теорема 10 [48]. *Для функции Шеннона $L_{\text{detect}}(n, Q(\Phi_{\vee}))$ при некоторой вещественной положительной константе C_2 справедлива нижняя оценка:*

$$L_{\text{detect}}(n, Q(\Phi_{\vee})) \geq C_2 \frac{2^n}{\sqrt{n}}.$$

Доказательство. Для удобства, говоря о слипаниях, будем подразумевать дизъюнктивные слипания. Будем говорить, что набор $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ переходит в набор $\tilde{\beta} = (\beta_1, \dots, \beta_n)$ в результате слипания переменных $x_{i_1}, \dots, x_{i_p}$, если $\beta_j = \alpha_{i_1} \vee \alpha_{i_2} \vee \dots \vee \alpha_{i_p}$ при $j \in \{i_1, \dots, i_p\}$ и $\beta_j = \alpha_j$ в противном случае.

Рассмотрим сначала нечетное n . Тогда $\left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{n}{2} \right\rfloor + 1$. Возьмем функцию $h(x_1, \dots, x_n)$, равную единице на всех наборах $\tilde{\alpha}$, для которых $|\tilde{\alpha}| = \left\lfloor \frac{n}{2} \right\rfloor$, и ну-

лю на всех остальных. Сузим класс возможных неисправностей до слипаний кратности $\left\lceil \frac{n}{2} \right\rceil$. В результате слипания переменных набор $\tilde{\beta}$ переходит в набор $\tilde{\beta}'$ так, что $|\tilde{\beta}'| \geq |\tilde{\beta}|$. Поэтому, если $|\tilde{\beta}| \geq \left\lceil \frac{n}{2} \right\rceil$, то на наборе $\tilde{\beta}$ значение любой из возможных функций неисправности равно нулю. Если $|\tilde{\beta}| < \left\lceil \frac{n}{2} \right\rceil$ и в слипании участвуют только переменные, на местах которых в наборе $\tilde{\beta}$ стоит ноль, данный набор не изменится и значение функции неисправности будет равно нулю. А если в слипании участвует хотя бы одна переменная, значение которой на наборе $\tilde{\beta}$ равно единице, тогда он перейдет в некоторый набор $\tilde{\beta}'$, для которого верно $|\tilde{\beta}'| \geq \left\lceil \frac{n}{2} \right\rceil$, в силу того, что кратность рассматриваемых слипаний равна $\left\lceil \frac{n}{2} \right\rceil$. Поэтому значение функций неисправности также будет равно нулю. Поэтому далее будем рассматривать только наборы $\tilde{\alpha} : |\tilde{\alpha}| = \left\lceil \frac{n}{2} \right\rceil$. Пусть $X' = \{x_{i_1}, \dots, x_{i_{\left\lceil \frac{n}{2} \right\rceil}}\}$, $X'' = \{x_{j_1}, \dots, x_{j_{\left\lceil \frac{n}{2} \right\rceil}}\}$, $X' \neq X''$. Тогда $h_{X'}^{x_{i_1} \vee \dots \vee x_{i_{\left\lceil \frac{n}{2} \right\rceil}}}$ и $h_{X''}^{x_{j_1} \vee \dots \vee x_{j_{\left\lceil \frac{n}{2} \right\rceil}}}$ — две различные функции неисправности.

Заметим, что если в наборе $\tilde{\alpha}$ есть хотя бы одна единица в позициях, соответствующих переменным из X' и хотя бы одна единица в позициях, соответствующих переменным из X'' , то обе функции будут равны нулю на данном наборе в силу кратности рассматриваемых слипаний. Тогда функции могут отличаться от нуля только на наборах, у которых в позициях $i_1, \dots, i_{\left\lceil \frac{n}{2} \right\rceil}$ или $j_1, \dots, j_{\left\lceil \frac{n}{2} \right\rceil}$ стоят все нули. Поскольку рассматриваются только наборы, в которых ровно $\left\lceil \frac{n}{2} \right\rceil$ единиц, получаем, что данные функции различаются всего на двух наборах.

Пусть в тест не входят два набора $\tilde{\alpha}'$ и $\tilde{\alpha}''$, для которых $|\tilde{\alpha}'| = |\tilde{\alpha}''| = \left\lceil \frac{n}{2} \right\rceil$. Тогда слипание переменных, соответствующих нулям в наборе $\tilde{\alpha}'$, и слипание переменных, соответствующих нулям в наборе $\tilde{\alpha}''$, не будут отличены друг от друга.

Отсюда следует, что в тест входит не менее, чем $C_n^{\left\lceil \frac{n}{2} \right\rceil} - 1$ наборов. Оценив данное выражение снизу и устремив n к бесконечности, получаем:

$L_{\text{diagn}}(n, Q(\Phi_{\vee})) \geq C_n^{\lfloor \frac{n}{2} \rfloor} - 1 > C_{n-1}^{\frac{n-1}{2}} \sim \frac{2^{n-1}}{\sqrt{\pi^{\frac{n-1}{2}}}} \sim \frac{1}{\sqrt{2\pi}} \frac{2^n}{\sqrt{n}}.$ Для чет-
ных n , рассматривая функцию $h(x_1, \dots, x_n)$, равную единице только на наборах
 $\tilde{\alpha} : |\tilde{\alpha}| = \frac{n}{2} - 1$, и слияния кратности $\frac{n}{2} + 1$, аналогично получаем нижнюю
оценку длины теста для выбранной функции: $L_{\text{diagn}}(n, Q(\Phi_{\vee})) \geq C_n^{\frac{n}{2}-1} - 1 >$
 $C_{n-2}^{\frac{n}{2}-1} \sim \frac{2^{n-2}}{\sqrt{\pi^{\frac{n-1}{2}}}} \sim \frac{1}{2\sqrt{2\pi}} \frac{2^n}{\sqrt{n}}.$ □

Глава 3

Тестирование булевых функций относительно вытеснения переменных

3.1 Основные определения и обозначения

Определим понятие вытеснения переменных. Пусть $f(x_1, \dots, x_n)$ — булева функция, формально зависящая от n переменных. Будем считать, что среди переменных $x_1, \dots, x_n$ есть некоторое количество *вытесняемых* переменных. Все остальные переменные назовем *вытесняющими*. Пусть $i_1, \dots, i_n$ — произвольная перестановка множества чисел $\{1, \dots, n\}$. Предположим, что переменные $x_{i_1}, \dots, x_{i_k}$ являются вытесняемыми. Тогда вместо $f(x_1, \dots, x_n)$ реализуется функция неисправности $g(x_1, \dots, x_n)$, получающаяся из $f(x_1, \dots, x_n)$ подстановкой вместо каждой вытесняемой переменной x_{i_j} ($1 \leq j \leq k$) произвольной булевой функции $\phi_j(x_{i_{k+1}}, \dots, x_{i_n})$ от вытесняющих переменных. Функции $\phi_j(x_{i_{k+1}}, \dots, x_{i_n})$ будем называть *функциями подстановки*. Заметим, что вытесняемые переменные являются фиктивными в получившихся функциях неисправности. Будем говорить о *вытеснении*, если среди переменных $x_1, \dots, x_n$ есть некоторое число вытесняемых переменных. Обозначим данный источник неисправностей как I . Для функции Шеннона длины проверяющего теста в данной главе находится асимптотическая оценка высокой степени точности, а для функции

Шеннона длины диагностического теста находится асимптотика. Также получено значение длины минимального проверяющего теста относительно вытеснения переменных для почти всех булевых функций.

3.2 Проверяющий тест

В данной части будет частично использоваться терминология, введенная в [27].

Триадой направлений i, j для $f(x_1, \dots, x_n)$ будем называть три булевых набора, в которых содержатся правильные ребра i -го и j -го направления для $f(x_1, \dots, x_n)$. Триады направлений i, j и k, t для $f(x_1, \dots, x_n)$ называются ортогональными, если i, j, k, t — попарно различные числа. Совокупность l попарно ортогональных триад для $f(x_1, \dots, x_n)$ называется *l -системой триад*. Будем называть l -систему триад *насыщенной*, если невозможно добавить к ней еще одну триаду так, чтобы получилась $(l + 1)$ -система триад.

Лемма 15. *Множество наборов T является проверяющим тестом для схемы, реализующей функцию $f(x_1, \dots, x_n)$, относительно вытеснения переменных тогда и только тогда, когда T — тест существенности для $f(x_1, \dots, x_n)$.*

Доказательство. Пусть T — тест существенности для $f(x_1, \dots, x_n)$. Если вытесняются только фиктивные переменные, то реализуется функция, не отличимая от исходной. Если же вытесняется существенная переменная x_i , то в функции неистинности $g(x_1, \dots, x_n)$ она фиктивна. Следовательно, на одном из наборов правильного ребра i -го направления $g(x_1, \dots, x_n)$ будет отличаться от $f(x_1, \dots, x_n)$.

Пусть теперь $T = \{(\alpha_1^1, \dots, \alpha_n^1), (\alpha_1^2, \dots, \alpha_n^2), \dots, (\alpha_1^p, \dots, \alpha_n^p)\}$ — проверяющий тест для $f(x_1, \dots, x_n)$, не являющийся тестом существенности. Без ограничения общности будем считать, что x_1 — существенная переменная $f(x_1, \dots, x_n)$, для которой в T нет правильного ребра. Пусть $\phi(x_2, \dots, x_n)$ — булева функция, равная

α_1^i на каждом наборе $(\alpha_2^i, \dots, \alpha_n^i)$, $1 \leq i \leq p$, и принимающая произвольные значения на остальных наборах. Тогда, если x_1 — единственная вытесняемая переменная и вместо нее подставляется $\phi(x_2, \dots, x_n)$, то данная неисправность не может быть обнаружена на множестве наборов T . $\square$

Лемма 16. Пусть x_r, x_s , $r \neq s$, — существенные переменные функции $h(x_1, \dots, x_n)$, причем x_s является фиктивной для $h(x_1, \dots, x_{r-1}, 0, x_{r+1}, \dots, x_n)$ или $h(x_1, \dots, x_{r-1}, 1, x_{r+1}, \dots, x_n)$. Тогда существует триада направлений r, s для $h(x_1, \dots, x_n)$.

Доказательство. Без ограничения общности будем считать, что $r = 1$, $s = 2$ и x_2 фиктивна для $h(0, x_2, \dots, x_n)$. Выберем правильное ребро направления 2 для $h(x_1, x_2, \dots, x_n)$. Поскольку x_2 фиктивна для $h(0, x_2, \dots, x_n)$, то выбранное ребро состоит из наборов вида $(1, 0, \alpha_3, \dots, \alpha_n)$, $(1, 1, \alpha_3, \dots, \alpha_n)$. В свою очередь на наборах $(0, 0, \alpha_3, \dots, \alpha_n)$, $(0, 1, \alpha_3, \dots, \alpha_n)$ функция $h(x_1, \dots, x_n)$ принимает одинаковые значения. Отсюда следует, что либо $(1, 0, \alpha_3, \dots, \alpha_n)$, $(0, 0, \alpha_3, \dots, \alpha_n)$, либо $(1, 1, \alpha_3, \dots, \alpha_n)$, $(0, 1, \alpha_3, \dots, \alpha_n)$ — правильное ребро направления 1. Предположим, что это $(1, 0, \alpha_3, \dots, \alpha_n)$, $(0, 0, \alpha_3, \dots, \alpha_n)$. Тогда искомая триада состоит из наборов $(1, 0, \alpha_3, \dots, \alpha_n)$, $(1, 1, \alpha_3, \dots, \alpha_n)$, $(0, 0, \alpha_3, \dots, \alpha_n)$. $\square$

Следующие определения будут даны в предположении, что для $f(x_1, \dots, x_n)$ существует насыщенная l -система триад направлений $1, 2, \dots, 2l$.

Пусть $i_1, \dots, i_{2l}$ — некоторая перестановка из элементов множества $\{1, 2, \dots, 2l\}$ и Q — множество переменных $x_{2l+1}, x_{2l+2}, \dots, x_n$. Обозначим через $f_{\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_t}}^{i_1, i_2, \dots, i_t}$ подфункцию функции $f(x_1, \dots, x_n)$, полученную подстановкой констант $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_t}$ вместо переменных $x_{i_1}, x_{i_2}, \dots, x_{i_t}$ соответственно.

Определим $\Pi(i_1, \dots, i_{2l}, Q)$ как последовательность функций $f_{\alpha_{i_1}}^{i_1}, f_{\alpha_{i_1}, \alpha_{i_2}}^{i_1, i_2}, \dots, f_{\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_{2l}}}^{i_1, i_2, \dots, i_{2l}}$, где константы $\alpha_1, \dots, \alpha_{2l}$ индуктивно определяются следующим образом. Положим $\alpha_{i_1} = 1$, если $f_1^{i_1}$ зависит существенно

от большего числа переменных из Q , чем $f_0^{i_1}$. В противном случае положим $\alpha_{i_1} = 0$. Положим $\alpha_{i_k} = 1$, если $f_{\alpha_{i_1}, \dots, \alpha_{i_{k-1}}, 1}^{i_1, \dots, i_{k-1}, i_k}$ зависит существенно от большего числа переменных из Q , чем $f_{\alpha_{i_1}, \dots, \alpha_{i_{k-1}}, 0}^{i_1, \dots, i_{k-1}, i_k}$. В противном случае положим $\alpha_{i_k} = 0$.

Если $f_{\alpha_{i_1}, \dots, \alpha_{i_{k-1}}, \alpha_{i_k}}^{i_1, \dots, i_{k-1}, i_k}$ существенно зависит от меньшего числа переменных из Q , чем $f_{\alpha_{i_1}, \dots, \alpha_{i_{k-1}}}^{i_1, \dots, i_{k-1}}$, то переменную x_{i_k} будем называть *сильной* переменной в $\Pi(i_1, \dots, i_{2l}, Q)$. В работе [27] доказана следующая лемма.

Лемма 17. Пусть для $f(x_1, \dots, x_n)$ построена насыщенная l -система триад направлений $1, 2, \dots, 2l$. Тогда $2^q \geq |Q|$, где q — число сильных переменных в $\Pi(i_1, \dots, i_{2l}, Q)$.

Все переменные из множества $\{x_{i_{k+1}}, \dots, x_{i_n}\}$, которые являются существенными для $f_{\alpha_{i_1}, \dots, \alpha_{i_{k-1}}}^{i_1, \dots, i_{k-1}}$, но фиктивными для $f_{\alpha_{i_1}, \dots, \alpha_{i_{k-1}}, \alpha_{i_k}}^{i_1, \dots, i_{k-1}, i_k}$, будем называть *спутниками* переменной x_{i_k} .

Теорема 11 [15]. Имеет место двойное неравенство

$$2n - \log_2 n - 2 \log_2 \log_2 n + O(1) \leq L_{\text{detect}}(n, I) \leq 2n - \log_2 n + O(1).$$

Доказательство. Начнем с верхней оценки. В силу леммы 15 достаточно найти верхнюю оценку длины минимального теста существенности. Поскольку для фиктивных переменных нет ребер, входящих в тест существенности, будем предполагать, что все переменные функции $f(x_1, \dots, x_n)$ существенны.

Пусть для $f(x_1, \dots, x_n)$ построена насыщенная l -система триад. Без ограничения общности будем считать, что множества направлений триад есть $\{1, 2, \dots, 2l\}$.

Выберем наименьшее натуральное p , такое, что $2^p \geq n - 2p$.

Если $l \geq p$, то множество наборов, состоящее из данной l -системы триад и правильных ребер направлений $2l + 1, 2l + 2, \dots, n$ будет иметь мощность не более $2n - p$. Доказательство завершено, поскольку $p = \log_2 n + O(1)$.

Пусть теперь $l < p$. Покажем, что в этом случае для $f(x_1, \dots, x_n)$ существует некоторая система триад, мощность которой асимптотически не меньше $\log n$.

Построим последовательность $\Pi(i_1, \dots, i_{2l}, Q)$. Через q обозначим число сильных переменных в данной последовательности. По лемме 17 получаем неравенство: $2^q \geq n - 2l$. Из определения числа p следует, что $2^{p-1} < n - 2(p - 1)$. Поскольку $l < p$, то $2^{p-1} < n - 2(l - 1) = n - 2l + 2$. Тогда $2^q + 2 > 2^{p-1} \geq \frac{1}{2}(n - 2p)$. Следовательно, $q \geq \log_2(n) + O(1)$. У каждой сильной переменной есть свой спутник среди переменных из Q . Пусть x_s — спутник сильной переменной x_{i_k} . Тогда можно применить лемму 16, взяв в качестве h функцию $f_{\alpha_{i_1}, \dots, \alpha_{i_{k-1}}}^{i_1, \dots, i_{k-1}}$. Получаем, что существует триада направлений i_k, s для $f(x_1, \dots, x_n)$. Значит, для каждой сильной переменной и ее спутника существует триада соответствующих направлений. Всякая переменная из Q может быть спутником не более чем одной сильной переменной. Отсюда следует, что существует q -система триад для $f(x_1, \dots, x_n)$.

Пусть $\{j_1, \dots, j_{2q}\}$ — направления, соответствующие данной q -системе триад. Множество наборов, состоящее из выбранной q -системы триад и одного правильного ребра для каждого направления из $\{1, \dots, n\} \setminus \{j_1, \dots, j_{2q}\}$, имеет мощность не более $2n - q$ и является тестом существенности для $f(x_1, \dots, x_n)$. Это завершает доказательство, поскольку $q \geq \log n + O(1)$.

Теперь перейдем к нижней оценке.

Воспользуемся некоторыми сведениями из теории кодирования. Все использованные определения и свойства кодов можно найти в [45].

Пусть $\sigma_1 \dots \sigma_r$ — некоторое двоичное слово, а $\sigma_1 \dots \sigma_r \eta_1 \dots \eta_s$ — его расширение до слова в равномерном двоичном коде, исправляющем одну ошибку. Данный код также называется кодом Хэмминга. Слово $\sigma_1 \dots \sigma_r$ соответствует информационным разрядам, а $\eta_1 \dots \eta_s$ — проверочным. Известно, что можно построить код Хэмминга, в котором s — это наименьшее число, такое, что $2^s \geq r + s + 1$.

Выберем именно такой способ кодирования, тогда $s \leq \lceil \log_2 r \rceil + 1$. Из свойств самокорректирующихся кодов следует, что расстояние между двумя кодовыми словами не меньше трех. Для указанных $\sigma_1, \dots, \sigma_r, \eta_1, \dots, \eta_s$ определим функцию $h_{\sigma_1, \dots, \sigma_r}(z_1, \dots, z_s) = z_1^{\eta_1} z_2^{\eta_2} \dots z_s^{\eta_s}$. Она будет использоваться как вспомогательная далее.

Аналогично верхней оценке будем оценивать длину минимального теста существенности T . Сначала отметим, что в работе [27] говорилось о существовании функции, для которой длина теста существенности будет не менее $2n - \log_2 n - O(\log_2 \log_2 n)$, однако доказательства данного факта приведено не было. Заявленная в теореме оценка не противоречит данному значению.

Для краткости обозначим $r = \lceil \log_2 n \rceil$, $s = \lceil \log_2 \log_2 n \rceil + 1$, $t = n - \lceil \log_2 n \rceil - \lceil \log_2 \log_2 n \rceil - 1$. Назовем $y_1, \dots, y_r$ адресными переменными, $z_1, \dots, z_s$ — хеш-переменными, а $x_1, \dots, x_t$ — информационными переменными. Напомним, что через $\delta(\alpha_1, \dots, \alpha_m)$ обозначается число $\sum_{i=0}^{m-1} \alpha_{m-i} 2^i$. Тогда каждому булеву набору $(\alpha_1, \dots, \alpha_m)$ взаимно однозначно соответствует число $\delta(\alpha_1, \dots, \alpha_m)$ из множества $\{0, 1, \dots, 2^m - 1\}$.

Определим функцию $g(y_1, \dots, y_r, z_1, \dots, z_s, x_1, \dots, x_t) =$

$$\bigvee_{\sigma_1, \dots, \sigma_r: \delta(\sigma_1, \dots, \sigma_r) < t} y_1^{\sigma_1} \dots y_r^{\sigma_r} h_{\sigma_1, \dots, \sigma_r}(z_1, \dots, z_s) x_{\delta(\sigma_1, \dots, \sigma_r)}.$$

Ясно, что в T найдется подмножество S , содержащее хотя бы одно правильное ребро для каждого направления, соответствующего адресным и информационным переменным функции g . Очевидно, что $|T| \geq |S|$. Найдем нижнюю оценку мощности множества S .

Всякий набор может входить в правильное ребро не более чем одной информационной переменной. Действительно, пусть $(\tilde{\alpha}, \tilde{\beta})$ — правильное ребро направления x_i , а $(\tilde{\alpha}', \tilde{\beta}')$ — правильное ребро направления x_j . Поскольку у данных наборов разные значения разрядов, соответствующих адресным переменным, никакие два из них не могут совпадать.

Будем говорить, что множество наборов обладает свойством A^j , $0 \leq j \leq r$, если оно содержит правильные ребра для всех информационных переменных и адресных переменных $y_1, \dots, y_j$. Множество, обладающее свойством A^0 , может не содержать правильные ребра адресных переменных. Пусть S^j — некоторое минимальное по мощности множество, обладающее свойством A^j . Покажем, что в множестве S^j нет правильного ребра для y_{j+1} . В силу минимальности S^j может содержать правильное ребро для y_{j+1} , если только каждый набор данного ребра принадлежит одному из правильных ребер для $x_1, \dots, x_t, y_1, \dots, y_j$. Пусть $(\tilde{\alpha}, \tilde{\beta})$ — правильное ребро направления y_{j+1} , причем $g(\tilde{\alpha}) = 0$, а $g(\tilde{\beta}) = 1$. Предположим, что оба набора содержатся в множестве S^j . Тогда существует набор $\tilde{\alpha}'$, соседний с $\tilde{\alpha}$ по одной из переменных $x_1, \dots, x_t, y_1, \dots, y_j$, причем $g(\tilde{\alpha}') = 1$. Адресные разряды наборов $\tilde{\beta}$ и $\tilde{\alpha}'$ находятся на расстоянии не более чем 2. Тогда из свойств кода Хэмминга следует, что значения хеш-переменных в наборах $\tilde{\beta}$ и $\tilde{\alpha}'$ отличаются. В то же время наборы $\tilde{\alpha}, \tilde{\beta}$ являются соседними по адресной переменной, а наборы $\tilde{\alpha}, \tilde{\alpha}'$ — по адресной или информационной. Следовательно, у всех трех наборов значения разрядов, соответствующих хеш-переменным, совпадают. Получаем противоречие. Значит, для переменной y_{j+1} нет правильного ребра в S^j .

Пусть $S^0, S^1, \dots, S^r$ — некоторые минимальные по мощности множества, обладающие свойствами $A^0, A^1, \dots, A^r$ соответственно. Ясно, что S^{j+1} обладает свойством A^j . Но минимальное множество со свойством A^j не может содержать правильное ребро направления $j+1$. Следовательно, $|S^{j+1}| > |S^j|$, откуда получаем $2t = |S^0| < |S^1| < \dots < |S^r| \leq |S|$, из чего следует, что $|S| \geq 2t + r$. Это завершает доказательство.

В заключение отметим, что для данной функции нетрудно построить тест существенности, на котором достигается нижняя оценка. □

Теперь покажем, что для проверяющего теста относительно вытеснения переменных не выполняется эффект Шеннона. Под эффектом Шеннона понимается ситуация, когда сложность почти всех булевых функций асимптотически равна функции Шеннона. Например, эффект Шеннона имеет место быть, когда под сложностью булевой функции понимается сложность ее реализации в классе схем из функциональных элементов или контактных схем [10].

Теорема 12 [16]. *Для почти всех булевых функций $L_{\text{detect}}(f, I) = n + 1$.*

Доказательство. Снова воспользуемся леммой 15 и будем оценивать длину теста существенности для почти всех функций. Начнем с верхней оценки. В работе [6] доказано, что для почти всех булевых функций проверяющий тест относительно инверсий не более, чем одной переменной, имеет длину 1. Предположим, что для некоторой булевой функции $f(x_1, \dots, x_n)$ данный тест состоит из набора $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ и $f(\tilde{\alpha}) = a$. Тогда если переменная x_i , $1 \leq i \leq n$, существенна, то $f(\alpha_1, \dots, \alpha_{i-1}, \bar{\alpha}_i, \alpha_{i+1}, \dots, \alpha_n) = \bar{a}$. В противном случае инверсия переменной x_i не была бы обнаружена. Но это означает, что $(\alpha_1, \dots, \alpha_n), (\alpha_1, \dots, \alpha_{i-1}, \bar{\alpha}_i, \alpha_{i+1}, \dots, \alpha_n)$ — правильное ребро i -го направления. Получаем, что если взять множество T , состоящее из набора $\tilde{\alpha}$ и всех соседних ему наборов по существенным переменным функции $f(x_1, \dots, x_n)$, то получим тест существенности для функции $f(x_1, \dots, x_n)$, а, значит, и полный проверяющий тест относительно вытеснения переменных. Мощность данного теста не превосходит $n + 1$.

Перейдем к нижней оценке. Воспользуемся фактом, что у почти всех булевых функций все переменные существенны. Пусть $f(x_1, \dots, x_n)$ — булева функция без фиктивных переменных и T — некоторый минимальный тест существенности для данной функции. Введем граф $G = (V, E)$, вершины которого взаимно однозначно соответствуют наборам из T . Если наборы, приписанные двум вершинам графа, являются соседними по i -й компоненте, то соединим данные

вершины ребром с пометкой i . Пусть E_i — множество ребер с пометкой i . Ясно, что $|E_i| \geq 1$, иначе T не было бы тестом существенности. Произвольным образом удалив из E_i все ребра, кроме одного, перейдем к множеству ребер E'_i . Выполним эту операцию для всех i , объединим все множества E'_i , получим новое множество ребер E' и перейдем к графу $G' = (V, E')$. Покажем, что в G' нет циклов. Предположим противное. Пусть вершины $v_1, \dots, v_p$ образуют простой цикл и этим вершинам сопоставлены наборы $\tilde{\alpha}_1, \dots, \tilde{\alpha}_p$. Допустим, что ребро (v_1, v_2) помечено числом j , а ребро (v_p, v_1) — отличным от j числом k . Поскольку вершины $v_2, \dots, v_p$ образуют цепь, ни одно ребро в которой не помечено числом j , ясно, что в j -х разрядах наборов $\tilde{\alpha}_2, \dots, \tilde{\alpha}_p$ стоит одно и то же число, отличное от j -го разряда набора $\tilde{\alpha}_1$. Но тогда наборы $\tilde{\alpha}_1, \tilde{\alpha}_p$ не могут быть соседними по переменной x_k . Получаем противоречие. Следовательно, G' — ациклический простой граф, тогда число вершин в нем равно числу ребер плюс число связных компонент. В графе G' n ребер и хотя бы одна связная компонента. Таким образом, $|V| \geq n + 1$, $|T| \geq n + 1$, что завершает доказательство теоремы. Теорема доказана.

□

3.3 Диагностический тест

Лемма 18. Пусть вершины n -мерного булева куба покрашены в черный и белый цвет так, что все вершины, находящиеся на расстоянии 1 и 2 от белой вершины, покрашены в черный цвет. Тогда число черных вершин асимптотически равно 2^n .

Доказательство. Выберем любые две различные белые вершины и рассмотрим шары радиуса 1 с центрами в данных вершинах. Выбранные шары не пересекаются, потому что их центры не могут находиться на расстояниях 1 и 2. Тогда

шаров с центрами в белых вершинах не более $\frac{2^n}{n+1}$. А следовательно, и белых вершин не более $\frac{2^n}{n+1}$. Это означает, что число черных вершин асимптотически равно 2^n . $\square$

Теорема 13 [15]. *Имеет место асимптотическое равенство*

$$L_{\text{diag}}(n, I) \sim 2^n.$$

Доказательство. Для линейной функции $l(x_1, \dots, x_n) = x_1 \oplus x_2 \oplus \dots \oplus x_n$ функциями неисправности являются всевозможные функции, имеющие хотя бы одну фиктивную переменную. Покажем, как получить функцию $g(x_{j_1}, \dots, x_{j_k})$, $k < n$. Пусть $Z = \{x_1, \dots, x_n\} \setminus \{x_{j_1}, \dots, x_{j_k}\}$. Подставим в $l(x_1, \dots, x_n)$ вместо одной из переменных множества Z функцию $g(x_{j_1}, \dots, x_{j_k}) \oplus x_{j_1} \oplus x_{j_2} \oplus \dots \oplus x_{j_k}$, а вместо остальных переменных множества Z — нули. Тогда будет реализовываться требуемая функция $g(x_{j_1}, \dots, x_{j_k})$.

Рангом элементарной конъюнкции назовем число букв в ней. Рассмотрим всевозможные конъюнкции ранга $n - 1$, составленные из переменных $x_1, \dots, x_n$. Каждая из них равна единице на каком-то одном ребре булева куба, при этом всякому ребру соответствует конъюнкция. Если для какого-то ребра оба его набора не войдут в тест, то соответствующая конъюнкция не будет отличаться от тождественного нуля. Следовательно, из каждых двух соседних наборов куба хотя бы один должен войти в тест. А значит, если некоторый набор не входит в тест, то все наборы, находящиеся на расстоянии 1 от него, должны войти в тест.

Предположим теперь, что набор $\tilde{\alpha}$ вошел в тест, а соседние с ним наборы $\tilde{\alpha}'$ и $\tilde{\alpha}''$ не вошли. Но тогда конъюнкция K_1 , равная единице только на ребре $(\tilde{\alpha}, \tilde{\alpha}')$, и конъюнкция K_2 , равная только единице на ребре $(\tilde{\alpha}, \tilde{\alpha}'')$, не будут отличаться на наборах теста. Отсюда следует, что набор, вошедший в тест, может иметь только один соседний набор, который не вошел в тест.

Объединяя эти два наблюдения, получаем, что если набор $\tilde{\beta}$ не входит в тест, то все наборы, находящиеся на расстоянии 1 и 2 от него, обязаны войти в тест. Действительно, пусть два набора, находящиеся на расстоянии 2, не входят в тест. Тогда их общий соседний набор входит в тест и при этом имеет два соседних набора, не вошедших в тест, что невозможно. Раскрасим булев куб так, что все вершины, вошедшие в тест, имеют черный цвет, а не вошедшие — белый. Тогда по лемме 18 получаем, что число наборов теста асимптотически равно 2^n . $\square$

Заключение

Изложенные в диссертации результаты относятся к теории тестирования входов схем. Для большинства рассматриваемых источников неисправностей изучены проверяющие и диагностические тесты. Функционалом качества тестирования является функция Шеннона, равная длине минимального теста самой сложнотестируемой функции.

Первые две главы посвящены источнику неисправностей типа слипания. В главе 1 рассматриваются линейные слипания. Для них получена асимптотика функции Шеннона длины проверяющего теста, а также ряд результатов для функции Шеннона длины диагностического теста. Также получены оценки, в ряде случаев асимптотические, для проверяющих и диагностических тестов относительно локальных k -кратных линейных слипаний.

В главе 2 изучаются монотонные симметрические слипания, являющиеся обобщением дизъюнктивных слипаний, и собственно дизъюнктивные слипания. Для монотонных симметрических слипаний получены нижняя линейная и верхняя квадратичная оценка функции Шеннона длины проверяющего теста, а также точное значение функции Шеннона длины диагностического теста. Для дизъюнктивных слипаний проверяющий тест был рассмотрен ранее Г.Р. Погосяном, в настоящей работе получена высокая нижняя оценка функции Шеннона длины диагностического теста.

Глава 3 посвящена вытесняющим неисправностям, которые являются обобщением константных неисправностей. Для проверяющего теста получена асимп-

тотическая оценка высокой степени точности функции Шеннона, а для диагностического теста найдена асимптотика функции Шеннона. Установлено точное значение длины проверяющего теста относительно вытесняющих неисправностей для почти всех булевых функций. Также в главе показано, что проверяющий тест относительно вытесняющих неисправностей является тестом существенности и наоборот. Отсюда следует, что соответствующие результаты справедливы и для теста существенности.

Литература

1. Беджанова С. Р. О минимальных тестах для схем, реализующих дизъюнкцию // Дискретный анализ и исследование операций. — 2008. — Т. 15, № 2. — С. 3-11.
2. Бородина Ю. В. О синтезе легкотестируемых схем в случае однотипных константных неисправностей на выходах элементов // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2008. — № 1. — С. 40-44.
3. Бородина Ю. В. О схемах, допускающих единичные тесты длины 1 при константных неисправностях на выходах элементов. // Вестник Московского университета. Серия 1. Математика. Механика. — 2008. — № 5. — С. 49-52.
4. Бородина Ю. В., Бородин П. А. Синтез легкотестируемых схем в базисе Жегалкина при константных неисправностях типа 0 на выходах элементов // Дискретная математика. — 2010. — Т. 22, № 3. — С. 127-133.
5. Глазунов Н. И., Горяшко А. П. Об оценках длин обнаруживающих тестов для классов неконстантных неисправностей входов комбинационных схем // Изв. АН СССР. Серия „Техническая кибернетика“. — 1986. — № 3. — С. 197-200.
6. Икрамов А. А. О сложности тестирования логических устройств на некоторые типы неисправностей // Интеллектуальные системы. — 2013. Т. 17, вып. 1-4. — С. 311-313.
7. Коваценко С. В. Синтез легкотестируемых схем в базисе Жегалкина для инверсных неисправностей. // Вестник Московского университета. Серия 1.

- Математика. Механика. — 2000. — Вып. 2. — С. 45-47.
8. Кудрявцев В. Б., Гасанов Э. Э., Долотова О. А., Погосян Г. Р. Теория тестирования логических устройств. — М.: Физматлит, 2006. — 160 с.
 9. Кузнецов И. А., Романов Д. С. О полных проверяющих тестах относительно локальных слипаний переменных в булевых функциях // Ученые записки Казанского университета. Серия Физико-математические науки. — 2009. — Т. 151, № 2. — С. 92-97.
 10. Ложкин С. А. Лекции по основам кибернетики: Учебное пособие. — М.: Изд. отдел ф-та ВМиК МГУ, 2004. — 256 с.
 11. Мадатян Х. А. Полный тест для неповторных контактных схем // Проблемы кибернетики — 1970. — Вып. 23. — С. 103-118.
 12. Морозов Е. В., Романов Д. С. О тестах относительно локальных линейных слипаний переменных в булевых функциях // Вестник Нижегородского университета им. Н. И. Лобачевского. — 2012. — № 5(2). — С. 153-158.
 13. Морозов Е. В. О тестах относительно множественных линейных слипаний переменных в булевых функциях // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2014. — № 1. — С. 22-25.
 14. Морозов Е. В. О тестах относительно множественных монотонных симметрических слипаний переменных в булевых функциях // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2014. — № 4. — С. 27-37.
 15. Морозов Е. В. О полных тестах относительно вытесняющих неисправностей входов схем // Вестник Московского университета. Серия 1. Математика. Механика. — 2015. — № 1. — С. 55-59.

16. Морозов Е. В. О тестах для почти всех булевых функций относительно некоторых неисправностей входов схем // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2015. — № 1. — С. 57-64.
17. Морозов Е. В., Романов Д. С. Проверяющие тесты для булевых функций при линейных локальных неисправностях входов схем // Дискретный анализ и исследование операций. — 2015. — Т. 22, № 1. — С. 49-61.
18. Морозов Е. В. О единичных диагностических тестах относительно слипаний переменных в булевых функциях // Прикладная математика и информатика: Труды факультета ВМК МГУ имени М. В. Ломоносова. — 2013. — № 44. — С. 103-113.
19. Морозов Е. В., Романов Д. С. О тестах относительно локальных линейных слипаний входов схем // Проблемы теоретической кибернетики. Материалы XVI Международной конференции (Нижний Новгород, 20-25 июня 2011 года). — Нижний Новгород: Издательство Нижегородского университета, 2011. — С. 330-334.
20. Морозов Е. В., Романов Д. С. О проверяющих тестах относительно множественных линейных слипаний переменных // Материалы XI Международного семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О. Б. Лупанова (Москва, МГУ, 18-23 июня 2012 г.). — М.: Издательство механико-математического факультета МГУ, 2012. — С. 144-147.
21. Морозов Е. В. О диагностических тестах относительно слипаний переменных в булевых функциях // Материалы IX молодежной научной школы по дискретной математике и ее приложениям. — М.: Издательство ИПМ РАН, 2013. — С. 85-88.

22. Морозов Е. В. О тестах относительно вытесняющих неисправностей входов схем // Тихоновские чтения: Научная конференция, Москва, МГУ имени М. В. Ломоносова, 28 октября - 1 ноября 2013 г.: Тезисы докладов. — М.: МАКС Пресс, 2013. — С. 77.
23. Морозов Е. В. Тесты для булевых функций относительно линейных и монотонных симметрических слияний переменных. // Тихоновские чтения: Научная конференция, 2014 г.: Тезисы докладов. — М.: МАКС Пресс, 2014. — С. 45-46.
24. Морозов Е. В. Тестирование схем, реализующих булевы функции, относительно вытесняющих неисправностей входов // Сборник тезисов XXI Международной научной конференции студентов, аспирантов и молодых учёных Ломоносов-2014, секция "Вычислительная математика и кибернетика". — М.: Издательский отдел факультета ВМК МГУ, 2014. — С. 40-41.
25. Морозов Е. В. О тестах для булевых функций относительно монотонных симметрических слияний переменных // Проблемы теоретической кибернетики. Материалы XVII международной конференции (Казань, 16-20 июня 2014 г.). — Казань: Отечество, 2014. — С. 213-215.
26. Нечипорук Э. И. О сложности вентильных схем, реализующих булевские матрицы с неопределёнными элементами // ДАН СССР. — 1965. — Т. 163, № 1. — С. 40-42.
27. Носков В. Н. О сложности тестов, контролирующих работу входов логических схем // Дискретный анализ. — Вып. 27. — Новосибирск: ИМ СО АН СССР, 1975. — С. 23-51.
28. Носков В. Н. Диагностические тесты для входов логических устройств // Дискретный анализ. — Вып. 27. — Новосибирск: ИМ СО АН СССР, 1974. — С. 72-83.

29. Носков В. Н. Об универсальных тестах для диагностики одного класса неисправностей комбинационных схем // Методы дискретного анализа в исследовании экстремальных структур. — 1979. — Вып. 33. — С. 41-52.
30. Нурмеев Н. Н. Об универсальных диагностических тестах для одного класса неисправностей комбинационных схем // Вероятностные методы и кибернетика. — 1982. — Вып. 18. — С. 73-76.
31. Погосян Г. Р. О проверяющих тестах для входов логических устройств. — М.: Издательство ВЦ АН СССР, 1982. — 57 с.
32. Редькин Н. П. Надежность и диагностика схем. — М.: Издательство Московского университета, 1992. — 192 с.
33. Редькин Н. П. О полных проверяющих тестах для контактных схем // Методы дискретного анализа в исследовании экстремальных структур. — 1983. — Вып. 39. — С. 80-87.
34. Редькин Н. П. О проверяющих тестах замыкания и размыкания // Методы дискретного анализа в исследовании экстремальных структур. — Вып. 39. — Новосибирск: ИМ СО АН СССР, Вып. 40. — Новосибирск: ИМ СО АН СССР, 1983. — С. 87-90.
35. Редькин Н. П. О полных проверяющих тестах для схем из функциональных элементов // Математические вопросы кибернетики. — Вып. 2. — М.: Наука, 1989. — С. 192-222.
36. Редькин Н. П. О схемах, допускающих короткие единичные диагностические тесты // Дискретная математика. — 1989. — Т. 1, вып. 3. — С. 71-76.
37. Редькин Н. П. О единичных диагностических тестах для однотипных константных неисправностей на выходах функциональных элементов // Вестник Московского университета. Серия 1. Математика. Механика. — 1992. — Вып. 5. — С. 43-46.

38. Редькин Н. П. О схемах, допускающих короткие тесты // Вестник Московского университета. Серия 1. Математика. Механика. — 1988. — № 2. — С. 17-21.
39. Романов Д. С. О синтезе схем, допускающих полные проверяющие тесты константной длины относительно произвольных константных неисправностей на выходах элементов // Дискретная математика. — 2013. — Т. 25, вып. 2. — С. 104-120.
40. Романов Д. С. Об оценках функции Шеннона длины единичных тестов относительно транспозиций переменных // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2007. — № 2. — С. 23-29.
41. Романов Д. С. Метод синтеза легкотестируемых схем, допускающих единичные проверяющие тесты константной длины // Дискретная математика. — 2014. — Т. 26, № 2. — С. 100-130.
42. Чашкин А. В. Лекции по дискретной математике. — М.: Издательство механико-математического факультета МГУ, 2007. — 259 с.
43. Чегис И. А., Яблонский С. В. Логические способы контроля электрических схем // Тр. МИАН СССР. — 1958. — Т. 51. — С. 270-360.
44. Яблонский С. В., Чегис И. А. О тестах для электрических схем // УМН. — 1955. — Т. 10, вып. 4(66). — С. 182-184.
45. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986. — 384 с.
46. Angluin D. Queries and concept learning // Machine Learning. — 1987. — V. 2, no 11. — P. 351-369.
47. Goldman S. A., Kearns M. J. On the complexity of teaching // Journal of Computer and System Sciences. — 1995. — V. 50, no 1. — P. 20-31.

48. Morozov E. V. Single-fault diagnostics tests for coalescences of variables in Boolean functions // Computational Mathematics and Modeling. — 2014. — V. 25, Issue 4. — P. 583-591.
49. Reddy S. M. Easily testable realization for logic functions // IEEE Trans. Comput. — 1972. — no 1. — P. 124-141.
50. Romanov D. S. Tests with respect to permutations of variables in Boolean functions // Computational Mathematics and Modeling. — 2013. — V. 24, Issue 4. — P. 558-565.
51. Romanov D. S. Diagnostic tests for local coalescences of variables in Boolean functions // Computational Mathematics and Modeling. — 2012. — V. 23, Issue 1. — P. 72-79.
52. Valiant L. G. A theory of the learnable // Communications of the ACM. — 1984. — V. 27. — P. 1134-1142.
53. Weiss S. D. Bounds on the length of terminal stuck-fault tests // IEEE Trans. Comput. V. C-21. — 1972. — no 3. — P. 305-309.