Московский государственный университет имени М. В. Ломоносова
Факультет вычислительной математики и кибернетики

На правах рукописи
УДК 519.718.7

Антюфеев Григорий Валерьевич

Оценки длин минимальных тестов для аргументов функций при подстановке констант, алгебраических операциях и сдвигах

Специальность 1.2.3. — «Теоретическая информатика, кибернетика»

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата физико-математических наук

Научный руководитель
доц., д.ф.-м.н.
Романов Дмитрий Сергеевич

Москва — 2024

Оглавление

Введение

Актуальность темы исследования. В настоящей диссертации отражены результаты исследований в области теории тестов, в которой поднимается проблема контроля исправности и диагностики неисправностей управляющих систем. Результаты теории тестов могут использоваться для создания систем тестирования сверхбольших интегральных схем. Ниже тема раскрывается более подробно.

Теория тестов и её приложения

Понятие «тест» используется во многих сферах человеческой деятельности. Одним из формальных подходов к изучению тестов является подход, реализованный в теории тестов (теории контроля управляющих систем) [43], которая является частью математической теории управляющих систем.

Под управляющими системами понимаются различные математические объекты, которые характеризуются структурой и функционированием. Следуя классикам, отметим, что широкий класс объектов может представлять собой управляющую систему. Например, арифметическое выражение, заданное некоторой формулой и представляющее некоторую арифметическую операцию, также является управляющей системой [23]. Существуют и другие примеры управляющих систем — это, например, схемы из функциональных элементов и контактные схемы [43]. В диссертации исследуются управляющие системы, функционирование которых описывается булевыми [45, 46] функциями.

Если функционирование объекта описывается функцией и его рассмотрение сводится только к рассмотрению данной функции без учёта внутренней структуры, то, как иногда говорят, объект представляет собой «чёрный ящик». Связь такого объекта с внешним миром осуществляется через полюса — входы и выходы [23].

Теория тестов была заложена Яблонским С. В. и Чегис И. А. в 1955 году [42]. Примерно в то же время изобретено устройство, для которого в будущем теория управляющих систем и вместе с ней теория тестов будут являться теоретической базой, — первая в мире микросхема [56, с. 1]. Также теория тестов находит приложение в задачах классификации и распознавания образов [8, 9, 15–18].

Тест — множество воздействий на управляющую систему, приводящее к отклику системы, по которому можно судить о её функционировании. Когда функционирование управляющей системы описывается булевой функцией, зависящей от n переменных, то воздействие — это набор значений (двоичных) этих переменных, а отклик — значения функции на этих наборах. Точно определить, какая функция описывает управляющую систему, возможно только полным перебором значений переменных, так как для любой функции существует функция, отличающаяся от неё только на одном наборе [18]. Для того чтобы можно было сделать какие-то выводы о функции и не перебирать всевозможные значения переменных, ограничивают число рассматриваемых объектов. Во-первых, можно проверять, что функция обладает каким-либо свойством, например, то, что функция принадлежит какому-то классу (обзор результатов в этом направлении представлен в докторской диссертации А. А. Вороненко [6]). Например, чтобы точно определить симметрическую функцию, достаточно выяснить её значения на $n + 1$ наборах, по одному с каждого слоя булева куба. Во-вторых, можно выбрать ограниченное множество функций, среди которых искать требуемую. Для ограничения множества

вводится понятие *неисправности* — чаще всего «небольшого» структурного изменения управляющей системы, потенциально приводящего к иному функционированию.

В диссертации рассматриваются управляющие системы без учёта внутренней структуры. В таком случае говорят, что *источник неисправностей действует на входы схем*, либо что *источник неисправностей (на входах схем) действует на булеву функцию*, либо что *неисправности действуют на аргументы (или переменные) функции*.

Стоит заметить, что для формализации модели неисправностей предполагается, что других неисправностей быть не может. То есть на переменные действуют неисправности какого-то определённого типа и только они. Можно сказать, что *тип неисправности* описывает множество возможных и чаще всего схожих структурных изменений управляющей системы. Например, если структурное изменение выбранного типа приводит к каким-то изменениям значений аргументов функции, то другие структурные изменения этого же типа могут отличаться лишь выбором аргументов, значения которых будут изменены. Если же требуется построить модель, где могут возникать неисправности и другого типа, то вводится понятие *разнотипных* или *смешанных* неисправностей и предполагается, что на переменные могут действовать неисправности разных типов, причём как по отдельности, так и одновременно.

Естественным образом возникает задача поиска воздействий, которые следует применить к исследуемой системе, чтобы по отклику точно определить наличие потенциальной неисправности (*проверяющие тесты*) и иногда получить дополнительную информацию, чтобы точно определить неисправность и соответствующую ей функцию (*диагностические тесты*). Так как, очевидно, перебор всевозможных воздействий (наборов значений) на систему не интересен, вопрос уточняется до поиска минимально возможного числа требуемых воздействий.

Исторически первый исследуемый тип неисправностей, немаловажный и в настоящее время, — это константные неисправности [39]. В микроэлектронике такие неисправности моделируют, например, замыкания на землю или питание, которые возникают на этапе производства [56, с. 677]. Также данная модель используется на этапе проектирования микроэлектронных устройств [44, с. 122]. В настоящее время использование модели константной неисправности особенно актуально для верификации систем повышенной надёжности [49, с. 12], причём как для функциональной верификации [52, с. 4], так и для формальной [48, с. 16] [47, с. 179]. Константные неисправности исследуются в первой главе настоящей диссертации.

Вторая глава посвящена алгебраическим неисправностям, которые выступают в качестве модели для задач мутационного тестирования программного обеспечения [53, с. 318].

Третья глава посвящена сдвиговым неисправностям.[1] Они могут использоваться в качестве модели ошибок, возникающих на этапе тестирования изготовленных микроэлектронных устройств, так как тестовые воздействия подаются во внутреннюю часть устройств посредством «задвигания» двоичных наборов [54, с. 423].

[1]Когда говорят о сдвиге, часто подразумевают операцию циклического сдвига. В диссертации речь идёт не о циклическом сдвиге, если не оговорено иное.

Обзор существующих результатов, близких к теме диссертации

В данном разделе приводятся основные результаты теории тестов для аргументов функций (входов схем). Речь будет идти о функциях, которые зависят от n аргументов. Уточним некоторые термины теории тестов и введём дополнительные.

Функция неисправности — это функция, получающаяся из исходной при возникновении неисправности.

Множество наборов значений аргументов функции является *проверяющим тестом* тогда и только тогда, когда по значениям функции на этих наборах можно с точностью до равенства функций[2] определить наличие неисправности, которая приводит к иному функционированию.

Множество наборов значений аргументов функции является *диагностическим тестом* тогда и только тогда, когда по значениям функции на этих наборах можно с точностью до равенства функций определить точный вид функции неисправности.

Количество наборов в тесте называется *длиной* теста. Ранее во введении было замечено, что интерес представляет минимально возможное число воздействий на исследуемую систему — это *тесты минимальной* длины.

Более того, если управляющая система описывается функцией, зависящей от n переменных, то встаёт вопрос о том, насколько вообще больши́м

[2]Возможно, что разные неисправности приводят к равным функциям неисправности или что исходная функция равна функции неисправности. Для того чтобы понимать, о чём идёт речь, в дальнейшем для каждой из функций будет использоваться своё обозначение. Например, рассматривается булева функция f и есть две неисправности, которые действуют на аргументы f и которым соответствуют функции неисправности f_1 и f_2. Таким образом, имеются три обозначения для функций, или для удобства говорится, что имеются три функции: f, f_1 и f_2. Однако допускается, что любые две из этих функций могут быть равны.

Ниже будут рассматриваться *таблицы неисправностей*, то есть такие таблицы, столбцы которых соответствуют векторам значений функций неисправности. Учитывая, что любые две функции неисправности могут быть равны, иногда мы будем рассматривать таблицы неисправностей с одинаковыми столбцами.

может быть минимальное число требуемых воздействий, если рассматривать всевозможные функции от n переменных, и как это число зависит от количества переменных. Такая зависимость получила название *функция Шеннона длины теста*.

Неисправности одного и того же типа отличаются значением какого-то параметра, например, выбором количества аргументов, значения которых изменяются. Естественно рассматривать следующие крайние случаи. Когда неисправность одна (или однократная), то используют термины *единичная неисправность* и *единичный тест*. Если же неисправностей может быть произвольное количество, то иногда используют термин *полный тест*.

Одними из первых исследуемых неисправностей были, как говорилось выше, *константные неисправности*. Несмотря на то что константные неисправности для контактных схем были введены в работе С. В. Яблонского и И. А. Чегис в 1955 году [42], данный тип неисправностей для входов схем впервые исследуется в работе К. Д. Вайса только в 1972 году [55]. Он рассматривает число переменных $n \geqslant 5$ и получает верхнюю оценку для функции Шеннона длины полного проверяющего теста, равную $2n - 4$. Далее, через три года В. Н. Носков доказывает [30], что при $t \geqslant 7$ эта функция Шеннона равна:

$$\begin{cases} 2n - 2t + 1, \text{ если } n = 2^{t-1} + t, \\ 2n - 2t, \text{ если } 2^{t-1} + t < n \leqslant 2^t + t. \end{cases}$$

Более того, В. Н. Носков показывает, что данная функция равна функции Шеннона для единичного проверяющего теста. Результат В. Н. Носкова был частично повторён, когда фактически в 1976 году (сноска в работе [51] о получении рукописи) Куль Д. Г. и Редди С. М. получают аналогичную нижнюю оценку. В 1982 году Погосян Г. Р. [33] показал, что результат можно обобщить до k-значных функций, и получил, что для любых $n \geqslant 1$ и $k \geqslant 2$

точное значение функции Шеннона следующее:

$$\begin{cases} 2n - 2t + 1, \text{ если } n = k^{t-1} + t, \\ 2n - 2t, \text{ если } k^{t-1} + t < n \leqslant k^t + t. \end{cases}$$

Носков В. Н. и Карповски М. с разных сторон подошли к изучению тестов для почти всех булевых функций. Носков В. Н. в ранее упоминавшейся статье 1975 года [30] доказал, что для почти всех функций существует единичный проверяющий тест длины 3, и установил линейность порядка длины минимального полного проверяющего теста. Карповски М. же ввёл понятие универсального теста [50], то есть такого множества наборов, который является тестом для почти всех функций одновременно. Он показал, что для единичных константных неисправностей длина минимального универсального теста асимптотически равна двум двоичным логарифмам от числа переменных.

Говоря про универсальность, стоит упомянуть результаты Носкова В. Н. и Нурмеева Н. Н., касающиеся уже́ диагностических тестов относительно любого преобразования (то есть не только константного) на не более чем k входах. Носков В. Н. показал, что в этом случае для почти всех булевых функций при постоянном k существует тест логарифмической длины от числа переменных [31], а Нурмеев Н. Н. — что при случайном выборе двоичных наборов, которые образуют множество, мощность которого есть логарифм по n, почти всегда получается диагностический тест [32].

В 1978 году Носков В. Н. рассматривает единичные неисправности [29] и получает точное значение для функции Шеннона длины теста, равное $2n$, и показывает, что почти для всех функций длина минимального теста асимптотически равна $\log n$. [3]

[3] В диссертации основание логарифма, равное двум, иногда опускается: $\log_2 n = \log n$.

В работе [28] Носков В. Н. получил оценки функции Шеннона для длины полного диагностического теста: верхняя оценка меньше либо равна $4(n+1)^3 \cdot 2^{0,773n}$, нижняя оценка больше либо равна $2^{\lfloor \frac{n}{2} \rfloor} - 1$. В 2016 году независимо появились два улучшения этой оценки. Автор настоящей диссертации улучшил оценку до величины, асимптотически равной $2^{\lfloor \frac{n}{2} \rfloor + 1}$ [60, 64] (теорема 2 настоящей диссертации). Попков К. А. получил [36], что при чётном n оценка будет $2^{n/2}$, а при нечётном n оценка будет $\left\lfloor \frac{2\sqrt{2}}{3} \cdot 2^{n/2} \right\rfloor$.

Ещё один из подходов к изучению константных неисправностей, рассмотрение однотипных константных неисправностей, подразумевает, что аргументы функции могут заменяться значением только одной заранее выбранной константы. В этом направлении Попковым К. А. в 2016 году [35, 36] получена нижняя оценка функции Шеннона длины полного диагностического теста $\frac{2^{n/2} \cdot \sqrt[4]{n}}{2\sqrt{n + 0{,}5 \log_2 n + 2}}$.

Морозов Е. В. рассмотрел следующее обобщение константных неисправностей, разделив аргументы булевой функции на вытесняемые и вытесняющие. Источник неисправностей подставляет вместо вытесняемых переменных произвольные функции, которые зависят только от вытесняющих переменных. Морозов Е. В. оценил поведение функции Шеннона длины полного проверяющего теста относительно такого источника как $2n - \log n \cdot (1 + o(1))$ и показал, что функция Шеннона длины диагностического теста асимптотически равна 2^n [25].

От константных перейдём к другому типу классических неисправностей — инверсным. В уже упоминавшейся работе [33] Погосян Г. Р., помимо константных неисправностей, рассматривает инверсные неисправности, которые заключаются в том, что значения аргументов функции могут быть инвертированы. Погосян Г. Р. устанавливает, что функция Шеннона длины проверяющего теста для случая единичных неисправностей равна $n - t$, где t определяется из равенства $2^{t-1} + t \leqslant n \leqslant 2^t + t$, а для произвольного числа

инверсий лежит в пределах от $n-1$ до n. Для полноты картины заметим: несложно видеть, что функция Шеннона полного диагностического теста равна $2^n - 1$. Нижняя оценка, например, фактически установлена в [2].

Один из подходов к изучению различного типа неисправностей заключается в рассмотрении наиболее общих неисправностей и в последующем переходе к частным случаям. По такому пути пошёл Романов Д. С., распространив методику Погосяна Г. Р. для получения верхних оценок. В работе [38] им была рассмотрена группа биекций относительно операции композиции на множестве всех возможных двоичных наборов длины n. Каждая биекция описывает неисправность следующим образом: каждый набор значений аргументов функции, на которую действует источник неисправностей, заменяется на соответствующий набор относительно выбранной биекции. Романов Д. С. показал, что функция Шеннона длины проверяющего теста относительного такого источника неисправностей ограничена сверху логарифмом от числа элементов группы. Отсюда, а также используя нижнюю оценку из работы [7], Романов Д. С. получает, что порядок функции Шеннона длины полного проверяющего теста относительно произвольных перестановок, а также перестановок и отрицаний переменных булевой функции равен $n \log n$. В той же работе для функций Шеннона длины диагностического теста относительно перестановок переменных получены следующие асимптотические оценки: для полного теста оценка 2^n, для теста относительно единичных транспозиций $\frac{n^2}{2}$. Лопунов М. А. [21] исследует функцию Шеннона длины проверяющего теста относительно перестановок любых k подряд идущих переменных функции и получает порядок её роста $n \log k$.

Автор диссертации рассматривает в своей работе источники неисправностей, которые действуют на аргументы в соответствии с алгебраическими операциями на выбранном кольце. По аналогии с понятием «легкотестируемости», используемым Бородиной Ю. В. [3], автор настоящей диссертации

вводит понятие *легкотестируемых* функций, то есть функций, порядок длины диагностических тестов которых равен логарифму от числа функций неисправности.[4] В работе [57] он описывает (теорема 11 и следствие 7 настоящей диссертации) легкотестируемые функции относительно сдвигов аргументов (с одновременной подстановкой *фиксированных* значений вместо сдвинутых аргументов).

Оценки функции Шеннона относительно сдвигов аргументов функции при подстановке *произвольных* значений вместо сдвинутых аргументов получены автором настоящей диссертации в [60, 63]: точная оценка 2 для проверяющего теста и порядок $2^{0,5n}$ для диагностического теста (теорема 7 и теорема 8 настоящей диссертации). Далее в 2019 году в работе [58] автор настоящей диссертации (теорема 10 диссертации) показал линейность функции Шеннона длины диагностического теста относительно сдвигов аргументов функции при замещении сдвинутых аргументов заранее выбранными фиксированными значениями.

Циклические сдвиги аргументов функций изучаются Курбацкой В. К. в работе [20]. Разбив переменные булевой функции на p непересекающихся подмножеств, Курбацкая В. К. получает следующие результаты. Функция Шеннона длины диагностического теста относительно циклического сдвига аргументов в подмножествах равна произведению мощностей подмножеств минус один. Также Курбацкая В. К. исследует смешанный источник неисправностей, в котором помимо циклических сдвигов в подмножествах переменных происходит однотипная единичная константная неисправность. Для такого источника неисправностей функция Шеннона длины диагностического теста линейна. Если рассматривать аргументы без разбиения на подмножества, то функция Шеннона длины проверяющего теста относительно циклического

[4] Заметим, что точная нижняя оценка длины диагностического теста для любого источника неисправностей равна целой части сверху от логарифма от числа попарно различных функций неисправности, включая исходную функцию.

сдвига аргументов функции при единичной однотипной константной неисправности больше либо равна n. Причём доля тех функций, для которых верхняя оценка аналогична, стремится к единице.

Ряд результатов, посвящённых проверяющим тестам относительно различных смешанных источников неисправностей, присутствует в диссертации Погосяна Г. Р. [34], а также сведён в книгу «Теория тестирования логических устройств» [17]. Показано равенство функций Шеннона длины полного проверяющего теста для константных неисправностей и для них же при единичной инверсной неисправности для $n \geqslant 1$. Также при $n \geqslant 1$ для функции Шеннона полного теста при константных неисправностях и инверсных неисправностях получена точная нижняя оценка, равная функции Шеннона длины полного теста для константных неисправностей, и верхняя, равная $2n$. Следующие результаты из работы [17] касаются в том числе и неисправностей типа слипания, при которых переменные делятся на множества и вместо переменных каждого множества подставляется максимальное (дизъюнктивные слипания) или минимальное (конъюнктивные слипания) значение переменных соответствующего множества. Далее в этом абзаце речь идёт о $n \geqslant 2$. Показаны следующие оценки функции Шеннона длины тестов для одновременного воздействия константных неисправностей и дизъюнктивных слипаний в k-значном случае и функции Шеннона длины тестов для одновременного воздействия константных неисправностей, дизъюнктивных слипаний и единичной инверсной неисправности в 2-значном случае: нижняя оценка равна функции Шеннона длины полного проверяющего теста для константных неисправностей при соответствующем k, а верхняя меньше либо равна $2n$. Для случая единичной инверсной неисправности и дизъюнктивных слипаний получена точная оценка функции Шеннона в диапазоне от $n - 1$ до n, которая впоследствии уточнена Икрамовым А. А. до точной оценки, равной

n [13], и, более того, показано, что оценка сохраняется, когда слипания не дизъюнктивные, а конъюнктивные.

Неисправности типа слипания (без смешивания с другими неисправностями) также были рассмотрены в работе [13] Икрамова А. А. Он получил, что функция Шеннона длины проверяющего теста при одновременно конъюнктивных и дизъюнктивных слипаниях равна $2(n-1)$. Заметим, что до этого для дизъюнктивных слипаний Погосяном Г. Р. было получено точное значение $n-1$ [33].

Порядок нижней оценки функции Шеннона длины единичного диагностического теста $\frac{2^n}{\sqrt{n}}$ при дизъюнктивных слипаниях установлен Морозовым Е. В. [27]. Им же в работах [24, 26, 27] получены оценки для следующих типов слипаний. Оценки для функции Шеннона длин полных проверяющих тестов: при линейных слипаниях функция Шеннона асимптотически равна $0,5n^2$, при монотонных симметрических слипаниях нижняя оценка $2n$ и верхняя оценка квадратична по порядку. Оценки для функции Шеннона длин полных диагностических тестов: при линейных слипаниях оценка равна n^2, при существенных линейных слипаниях верхняя асимптотическая оценка равна $2^{0,773n}$, при монотонных симметрических слипаниях точное значение равно 2^n. При $2 \leqslant k \leqslant n$ и $t = 2^{2^k}$ Романов Д. С. и Кузнецов И. А. установили оценки функции Шеннона длины единичного проверяющего теста относительно локальных k-местных слипаний: нижняя $2^{k-1}(n-k+2)$, верхняя $(2^{k-1}+1)\cdot(n-k+1)+2^k\left\lceil\frac{n-k+1}{k}\right\rceil$ [19]. Для диагностического теста при $n \to \infty$, $k = k(n) \to \infty$ и $2 \leqslant k \leqslant n$ Романов Д. С. получил асимптотическое поведение равное $2^k(n-k+1)$ [37].

Приведённый обзор результатов демонстрирует преемственность подходов к исследованиям и показывает, что, возникнув более полувека назад, теория тестов является проработанной теорией. Для того чтобы провести более полное исследование тестов, прибегают к различным постановкам

задач: получение оценок функции Шеннона, анализ почти всех функций относительно выбранного источника неисправностей, нахождение универсальных тестов, описание легкотестируемых функций. Наряду с различными типами неисправностей, рассматриваются также и разнотипные неисправности. В некоторых случаях используется дифференциация, посредством введения понятия кратности. Иногда, наоборот, используется обобщение.

Определения и обозначения

В данном разделе вводятся понятия из различных областей математики, в том числе из теории тестов. Дополнительную информацию по теории тестов можно найти в книгах [22, 43].

В качестве инструментов в теории тестов используется булева алгебра и перечислительная комбинаторика, информацию по ним можно получить в книге [41].

Для операции умножения (в том числе при работе с кольцами) используется стандартный символ «·», который также иногда может опускаться. Для обозначения классов вычетов в диссертации используется готический шрифт.

Множество A является *подмножеством* множества B, если все элементы A являются элементами B. Это будет обозначаться $A \subset B$ или $B \supset A$. Если A — подмножество B, не равное всему B, то A называют *собственным* подмножеством B. Это будет обозначаться $A \subsetneq B$ или $B \supsetneq A$ [5].

Введём классические обозначения для некоторых множеств. Натуральные числа: $\mathbb{N} = \{1, 2, 3, \dots\}$. Целые неотрицательные числа: $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$. Целые числа: $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$. Положим $E_2 = \{0, 1\}$. Множество всех k-разрядных двоичных наборов $\tilde{\alpha}^k$: E_2^k.

Двоичная функция, определённая на множестве X, — это функциональное соответствие $X \to \{0, 1\}$. Пусть для двоичной функции f множество X равно E_2^n, тогда функция f является *булевой функцией, которая зависит от переменных* $x_1, x_2, \dots, x_n$. Это обозначается следующим образом: $f(x_1, x_2, \dots, x_n)$ или $f(\widetilde{x}^n)$. Часто в тех местах, которые не приводят к неоднозначности, обозначения для переменных опускаются, и пишется просто f. Множество булевых функций от n переменных обозначается через P_2^n. Булева функция $f(x_1, x_2, \dots, x_n)$ однозначно определяется своим *характери-*

стическим множеством, которое состоит из всех наборов $\tilde{\alpha} \in E_2^n$ таких, что $f(\tilde{\alpha}) = 1$. Характеристическое множество функции f обозначается N_f.

Два k-разрядных двоичных набора $\tilde{\alpha}^k$ и $\tilde{\beta}^k$, $\tilde{\alpha}^k, \tilde{\beta}^k \in E_2^k$, называются *соседними*, если они различаются только в одном i-ом разряде, $i = 1, \ldots, k$. При рассмотрении булевых функций также говорят, что наборы являются *соседними по переменной* x_i.

Переменная x_i, $i = 1, \ldots, n$, называется *существенной переменной* функции $f(x_1, x_2, \ldots, x_n) \in P_2^n$, если существуют такие соседние по x_i значения $\tilde{\alpha} \in E_2^n$ и $\tilde{\beta} \in E_2^n$ переменных $x_1, x_2, \ldots, x_n$, что $f(\tilde{\alpha}) \neq f(\tilde{\beta})$. Если x_i не является существенной переменной, то она называется *фиктивной*. Говорят, что функция f *существенно зависит от переменной* x_i, если x_i — существенная переменная функции f.

Будем говорить, что булева функция $g'(x_1, x_2, \ldots, x_n)$ *линейно зависит от* x_i, если $g'(\tilde{\alpha}) \neq g'(\tilde{\beta})$ для любых соседних по x_i наборов $\tilde{\alpha}, \tilde{\beta} \in E_2^n$.

Функции x и $\bar{x}$ называются буквами переменной x. Также будем использовать следующие обозначения $x^0 = \bar{x}$, $x^1 = x$. Конъюнкция букв различных переменных называется *элементарной конъюнкцией*.

Положим $E_3 = \{0, 1, *\}$ и пусть $\tilde{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n) \in E_3^n$. *Грань* $\tilde{\varepsilon}$ — множество всех тех наборов $\tilde{\alpha} \in E_2^n$, для которых $\alpha_i = \varepsilon_i$ при всех $i = 1, \ldots, n$ таких, что $\varepsilon_i \neq *$.

При рассмотрении асимптотического поведения функций речь будет идти о действительнозначных функциях целого неотрицательного аргумента, который стремится к бесконечности. Для этого используются следующие понятия и обозначения [12, 14, 41].

Положим $f(x) = O(g(x))$, если существуют такие положительные константы C, x_0, что верно $|f(x)| \leqslant Cg(x)$ для всех $x \geqslant x_0$. Положим $f(x) = \Omega(g(x))$, если существуют такие положительные константы C, x_0, что

верно $Cg(x) \leqslant |f(x)|$ для всех $x \geqslant x_0$. Если $f(x) = O(g(x))$ и одновременно $f(x) = \Omega(g(x))$, то используется запись $f(x) = \Theta(g(x))$.

Положим $g(x) = o(f(x))$, если для любого $\varepsilon > 0$ найдётся такое положительное число x_0, что $|g(n)| < \varepsilon f(n)$ при всех $x \geqslant x_0$.

Введённые обозначения могут использоваться в формулах. По сути они обозначают множество функций. Таким образом, запись вида $f(x) = g(x)(1 + o(1))$ при $x \to \infty$ фактически означает, что $\frac{f(x)}{g(x)} \to 1$ при $x \to \infty$.

Функция, обозначаемая $\lfloor\, x \,\rfloor : \mathbb{R} \to \mathbb{Z}$, — это наибольшее целое число, которое не превосходит x. Функция, обозначаемая $\lceil\, x \,\rceil : \mathbb{R} \to \mathbb{Z}$, — это наименьшее целое число, которое не меньше x.

Пусть функционированием управляющей системы является булева функция f. *Источником неисправностей U, действующим на f*, формально можно считать конечное множество отображений $P_2^n \to P_2^n$, каждое из которых характеризуется некоторыми параметрами (например, позицией переменной). Применим устоявшийся описательный подход к определению источника неисправностей. Перед описанием стоит заметить, что используются следующие синонимичные словосочетания, когда говорят про действие источника неисправностей, — источник неисправностей действует: a) на функцию; b) на аргументы (или на переменные) функции; c) на входы схемы.

Если функция f преобразуется в функцию f' из какого-то множества функций F_U, то говорят, что на функцию *действует источник неисправностей U*. Множество F_U характеризует источник неисправностей U. Это множество формируется на основе функции f, при неисправностях (изменениях) на её аргументах в соответствии с U. В каждом исследуемом случае неисправности будут описываться явно. Будем считать, что F_U также включает в себя исходную функцию f. Также множество может формироваться на основе таблицы векторов значений функций. Такая таблица называется

таблицей неисправностей. Она, в свою очередь, может быть дана изначально, либо может формироваться на основе F_U. Таким образом, возникает очевидная биекция между таблицами неисправностей и F_U. Функция f' называется *функцией неисправности* или *функцией, порождённой источником неисправностей* U.

Таблица неисправностей называется *отделимой по столбцам*, если все её столбцы различны.

Множество T наборов значений переменных $x_1, x_2, \ldots, x_n$ называется *(полным) проверяющим тестом относительно источника неисправностей* U, *действующего на функцию* f, тогда и только тогда, когда для любой функции $g\left(\widetilde{x}^n\right) \in F_U$ такой, что $g\left(\widetilde{x}^n\right) \neq f\left(\widetilde{x}^n\right)$, найдётся набор $\widetilde{a}$ из T, для которого выполнено неравенство $f\left(\widetilde{a}\right) \neq g\left(\widetilde{a}\right)$.

Множество T наборов значений переменных $x_1, x_2, \ldots, x_n$ называется *диагностическим тестом относительно источника неисправностей* U, *действующего на функцию* f, тогда и только тогда, когда для любых двух неравных функций g и h, порождённых источником U (также в качестве одной из этих функций может быть выбрана исходная функция f), найдётся набор $\widetilde{a}$ из T, для которого выполнено неравенство $g\left(\widetilde{a}\right) \neq h\left(\widetilde{a}\right)$.

Длина теста $L(T)$ — это мощность T. Тест минимальной длины называется *минимальным*. Обозначим через $L^{\text{detect}}(U, f\left(\widetilde{x}^n\right))$ (соответственно, через $L^{\text{diagn}}(U, f\left(\widetilde{x}^n\right))$ длину минимального полного проверяющего (соответственно, диагностического) теста относительно источника неисправностей U, действующего на функцию $f\left(\widetilde{x}^n\right)$.

Функции Шеннона длины (полного) проверяющего и диагностического теста относительно источника неисправностей U:

$$L^{\text{detect}}\left(U, n\right) = \max_{f\left(\widetilde{x}^n\right) \in P_2^n} L^{\text{detect}}\left(U, f\left(\widetilde{x}^n\right)\right),$$

$$L^{\text{diagn}}\left(U, n\right) = \max_{f\left(\widetilde{x}^n\right) \in P_2^n} L^{\text{diagn}}\left(U, f\left(\widetilde{x}^n\right)\right).$$

Пусть $n_i \to \infty$ при $i \to \infty$. Тогда последовательность функций $f_i(x_1, x_2, \ldots, x_{n_i})$ будем называть *легкотестируемой относительно источника неисправностей* U, если порядок длины диагностического теста относительно U, действующего на $f_i(x_1, x_2, \ldots, x_{n_i})$, равен логарифму по основанию два от числа попарно неравных столбцов соответствующей таблицы неисправности. В ряде случаев будем и к функциям из этой последовательности применять термин *легкотестируемая функция*.

Далее вводятся необходимые определения из общей алгебры. Дополнительные определения из общей алгебры можно найти в книгах [1, 4, 10].

Коммутативное кольцо A — множество с двумя бинарными операциями (сложение и умножение), которое удовлетворяет следующим аксиомам:

1. По сложению A является абелевой группой.

2. Умножение ассоциативно: $(xy)z = x(yz)$ и дистрибутивно относительно сложения: $x(y+z) = xy + xz,\ (y+z)x = yx + xz$.

3. Для всех x, $y \in A$ выполняется $xy = yx$.

4. Существует такой элемент $1 \in A$, что $x1 = 1x = x$ для всех $x \in A$. Элемент 1 называется *единицей кольца* A *или единичным элементом кольца* A.

Конечное кольцо — кольцо, множество которого конечно. В диссертации термин *кольцо* будет означать конечное коммутативное кольцо. *Таблица Кэли для операции умножения кольца* A (далее просто *таблица Кэли*) — таблица, строки и столбцы которой индексированы элементами кольца A, а в каждой клетке записан результат применения операции умножения кольца A к элементам, соответствующим строке и столбцу.

Порядок кольца — количество элементов кольца. Порядок кольца A обозначается $|A|$.

Пусть $B, C \subset A$, тогда $B + C \subset A$ и состоит из всех элементов $b + c$, а $BC \subset A$ и состоит из всех элементов bc, $b \in B, c \in C$. При сложении или умножении с одноэлементным подмножеством $\{x\}$ фигурные скобки иногда могут опускаться.

Идеал I в кольце A — аддитивная подгруппа со свойством $AI \subset I$. Пусть $x \in A$, тогда все кратные xa некоторого элемента $a \in A$ образуют идеал, который обозначается (a) и называется *главным*. *Кольцо главных идеалов* — кольцо, каждый идеал которого главный.

Произведение главных идеалов (a) и (b) — это идеал (ab), то есть $(a) \cdot (b) = (ab)$ (см., например, [4, с. 426]). Степень $(a)^n$ главного идеала (a) определяется так: $(a)^1 = (a), (a)^{n+1} = (a) \cdot (a)^n$, где $n \in \mathbb{N}$. Положим $(a)^0 = (a^0) = (1) = A$.

Нулевой идеал (0) может обозначаться 0. *Простой идеал* — такой идеал I кольца A, что $I \neq A$ и из $cb \in I$ следует $b \in I$ или $c \in I$. *Максимальный идеал* кольца A — всякий собственный идеал кольца, не содержащийся ни в каком другом собственном идеале.

Специальное кольцо — кольцо главных идеалов, имеющее только один простой идеал $I \neq A$ и $I^{n'} = (0)$ для некоторого $n' \in \mathbb{N}$.

Формулировка полученных результатов и структура диссертации

Степень разработанности темы исследования

Степень разработанности темы исследования является высокой, что отражено выше, в разделе «Обзор существующих результатов, близких к теме диссертации». В числе открытых вопросов теории тестов есть те, которые относятся к ранее не исследованным источникам неисправностей: одна часть вопросов связана с классическими моделями, другая часть возникла под влиянием практики. Некоторые из этих вопросов сформулированы в виде задач диссертации ниже в разделе «Цели и задачи диссертации».

Цели и задачи диссертации

Целью диссертации является получение оценок функций Шеннона длин диагностических и проверяющих тестов для аргументов функций относительно неисправностей некоторых типов.

Задачами диссертации являются:

- получение оценок функций Шеннона длин диагностических тестов относительно константных неисправностей и локальных константных k-кратных неисправностей аргументов булевых функций;
- получение оценок функций Шеннона длин проверяющих тестов относительно локальных константных k-кратных неисправностей аргументов булевых функций;
- получение оценок функций Шеннона длин диагностических и проверяющих тестов относительно сдвигов аргументов булевых функций;
- выделение некоторых классов легкотестируемых функций относительно источников неисправностей специального вида;

- получение оценок функций Шеннона длин диагностических тестов относительно источников неисправностей над некоторыми кольцами;
- получение оценок функций Шеннона длин диагностических тестов относительно сдвигов аргументов булевых функций на k позиций и относительно сдвигов аргументов булевых функций с фиксированным замещающим набором.

Объект и предмет исследования

Объект исследования диссертации — булевы функции. Предмет исследования — построение тестов некоторых типов для входов схем, реализующих булевы функции. Объект и предмет исследований диссертации, а так же её содержание **соответствуют паспорту специальности** 1.2.3 – «Теоретическая информатика, кибернетика» (физико-математические науки): полученные в ней результаты соотносятся с разделами «3. Теория сложности алгоритмов и вычислений (физико-математические науки)» и «5. Теория автоматов (физико-математические науки)» указанного паспорта специальности.

Научная новизна

Все результаты диссертации являются новыми и получены автором диссертации самостоятельно. Все оценки улучшают существующие или получены впервые. Во всех статьях [59, 60, 63, 64], совместно опубликованных автором с Романовым Д. С., постановка задач принадлежит Романову Д. С., результаты получены автором настоящей диссертации.

Теоретическая и практическая значимость работы

Работа, проделанная во время исследований, и её результаты являются теоретическими. Результаты могут применяться в дальнейших теоретических

исследованиях. Метод, разработанный для получения оценок некоторых легкотестируемых функций и их описания, может использоваться для изучения ранее не исследованных типов неисправностей. Практическая значимость работы обусловлена тем, что теория тестов является теоретической базой для тестирования цифровых устройств.

Методология и методы исследования

Методология исследования основывается на дискретной математике, математической кибернетике, комбинаторике, комбинаторике слов и абстрактной алгебре.

Положения, выносимые на защиту

Основные положения данной диссертации, выносимые на защиту, представляют собой результаты исследований тестов (а именно длин минимальных тестов и функций Шеннона длин минимальных тестов), с помощью которых обнаруживается и диагностируется действие следующих типов источников неисправностей (и их модификаций), действующих на аргументы булевых функций: константных неисправностей, сдвиговых неисправностей, мультипликативных неисправностей (формально определения различных источников неисправностей приводятся ниже). Результаты оформлены в виде математических утверждений и их доказательств.

Результаты, выносимые на защиту, опубликованы в работах [57–64]. Работы [57–60] изданы в журналах, которые входят в базу ядра Российского индекса научного цитирования "eLibrary Science Index".

На защиту выносятся следующие основные положения, которые подтверждаются результатами исследования. Получены:

1. оценки функции Шеннона длины диагностического теста относительно локальных k-кратных константных неисправностей на входах схем;

2. асимптотически оптимальные при некоторых ограничениях на n и k оценки функции Шеннона длины проверяющего теста относительно локальных k-кратных константных неисправностей на входах схем;

3. оптимальная по порядку роста нижняя оценка функции Шеннона длины диагностического теста относительно мультипликативного источника неисправностей над специальным кольцом, порядок которого есть степень двойки;

4. утверждение о связи между отделимостью таблиц неисправностей функции относительно всех мультипликативных источников неисправностей с аддитивными элементами над кольцом вычетов по модулю 2^n и длинами минимальных диагностических тестов для этой функции;

5. утверждение о точном значении функции Шеннона длины проверяющего теста относительно произвольных сдвигов аргументов;

6. утверждения об оптимальных по порядку роста оценках функции Шеннона длины диагностического теста относительно произвольных сдвигов аргументов;

7. утверждение об отличающихся не более чем на 1 оценках функции Шеннона длины диагностического теста относительно произвольных сдвигов аргументов на k позиций влево;

8. утверждение об оптимальной по порядку роста нижней оценке функции Шеннона длины диагностического теста относительно сдвигов аргументов влево с фиксированным замещающим набором;

9. утверждение о достаточном условии диагностической легкотестируемости функции относительно сдвигов аргументов влево с фиксированным замещающим набором.

Структура диссертации и объём диссертации

Диссертация состоит из введения, трёх глав, заключения и списка литературы. Текст изложен на 97 страницах, включая 3 таблицы. Список литературы включает 64 наименования.

Введение включает четыре раздела: «Теория тестов и её приложения», «Обзор существующих результатов, близких к теме диссертации», «Определения и обозначения», «Формулировка полученных результатов».

В диссертации используются следующие математические утверждения: теоремы, леммы и следствия. Нумерация всех типов утверждений сквозная, причём она независима для разных типов утверждений. Все доказываемые в диссертации теоремы и следствия приведены во введении с той же нумераций, что и в последующих главах, где формулировки теорем и следствий приводятся рядом с соответствующими доказательствами.

В **первой** главе представлены результаты исследований исторически первого источника неисправностей — источника константных неисправностей. Опишем константные источники неисправностей.

Источник U^{c} константных неисправностей действует на булеву функцию $f(x_1, x_2, \ldots, x_n)$ следующим образом. Источником выбираются переменные из списка $x_1, x_2, \ldots, x_n$, и вместо выбранных переменных производится подстановка констант из E_2.

Пусть $k \in \{1, \ldots, n\}$. Источник U_k^{lc} *локальных константных k-кратных неисправностей* действует на булеву функцию $f(x_1, \ldots, x_n)$ следующим образом. Источником выбирается двоичный набор $\widetilde{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_k) \in E_2^k$, где $k \leqslant n$, а также натуральное число m, $1 \leqslant m \leqslant n - k + 1$, и вместо вычисления $f(x_1, \ldots, x_m, \ldots, x_{m+k-1}, \ldots, x_n)$ происходит вычисление $f(x_1, \ldots, x_{m-1}, \varepsilon_1, \ldots, \varepsilon_k, x_{m+k}, \ldots, x_n)$.

Для локальных константных k-кратных неисправностей получены следующие утверждения.

Теорема 1 (Антюфеев Г. В. [60, 64])**.** *Для k, n, таких что $1 \leqslant k \leqslant n/2$, справедливо неравенство:*

$$L^{\mathrm{diagn}}\left(U_k^{\mathrm{lc}}, n\right) \geqslant \frac{2^{k+1}(n-k+1)-2}{(n-k+2)}.$$

Следствие 1 (Антюфеев Г. В. [60, 64])**.** *При $n \to \infty, k = k(n) \to \infty$, $1 \leqslant k \leqslant n/2, \log_2 n = o(k)$, справедливо асимптотическое равенство:*

$$\log_2 L^{\mathrm{diagn}}(U_k^{\mathrm{lc}}, n) = k(1 + o(1)).$$

Из того, что функции неисправности, которые получаются при действии источника локальных k-кратных константных неисправностей на функцию f, принадлежат множеству функций неисправности, порождённых источником U^{c}, следует теорема 2. Данная теорема поднимает нижнюю оценку функции Шеннона длины диагностического теста относительно источника константных неисправностей, полученную Носковым В. Н. в 1974 году [28].

Теорема 2 (Антюфеев Г. В. [60, 64])**.** *При $n \to \infty$ справедливо асимптотическое неравенство:*

$$L^{\mathrm{diagn}}(U^{\mathrm{c}}, n) \geqslant 2 \cdot 2^{\left\lfloor \frac{n}{2} \right\rfloor}(1 + o(1)).$$

Порядок функции Шеннона длины диагностического теста относительно k-кратных неисправностей получается в следствии из следующей теоремы.

Теорема 3 (Антюфеев Г. В. [59]). *Пусть n и k — целые положительные, $c > 1$ — действительная константа, $2 \leqslant k \leqslant \frac{n}{2c}$. Тогда имеют место неравенства:*

$$(n - 2k + 3 - \lceil \log_2(n - k + 1) \rceil) \cdot 2^{k-2} - 1 \leqslant L^{\mathrm{diagn}}(U_k^{\mathrm{lc}}, n) \leqslant (n - k + 1) \cdot 2^k.$$

Следствие 2 (Антюфеев Г. В. [59]). *Пусть n и k — целые положительные, $c > 1$ — действительная константа, $n \to \infty$, $2 \leqslant k \leqslant \frac{n}{2c}$, $k = k(n)$. Функция Шеннона длины диагностического теста относительно локальных k-кратных константных неисправностей имеет следующий порядок роста:*

$$L^{\mathrm{diagn}}(U_k^{\mathrm{lc}}, n) = \Theta(n2^k).$$

Для проверяющего теста относительно k-кратных неисправностей получены следующие оценки.

Теорема 4 (Антюфеев Г. В. [59]). *Пусть n и k — целые положительные, $2 \leqslant k \leqslant n$. Тогда имеют место неравенства:*

$$2 \cdot \left(\left\lfloor \frac{2 \cdot \left(n - \left\lceil \log_2 \left\lfloor \frac{2n}{k+1} \right\rfloor \right\rceil \right)}{k+1} \right\rfloor - 2 \right) \leqslant L^{\mathrm{detect}}(U_k^{\mathrm{lc}}, n) \leqslant 4 \cdot \left\lceil \frac{n+2}{k+1} \right\rceil - 4.$$

Следствие 3 (Антюфеев Г. В. [59]). *Пусть n и k — целые положительные, $n \to \infty$, $2 \leqslant k \leqslant n$, $k = k(n)$, $k = o(n)$. Тогда имеет место асимптотическое равенство:*

$$L^{\mathrm{detect}}(U_k^{\mathrm{lc}}, n) = \frac{4n}{k+1} \cdot (1 + o(1)).$$

Во **второй** главе исследуются неисправности, возникающие вследствие алгебраических операций, которые изменяют значения аргументов функций.

Пусть выбрано кольцо A, такое что $|A| = 2^n$, и задана биекция $\nu_A : E_2^n \to A$. Обратное отображение к ν_A — это отображение $\nu_A^{-1} : A \to E_2^n$, такое что $\nu_A(\nu_A^{-1}(a)) = a$ для всех $a \in A$, и $\nu_A^{-1}(\nu_A(\tilde{\alpha}^n)) = \tilde{\alpha}^n$ для всех $\tilde{\alpha}^n \in E_2^n$. Введём источник неисправностей, таблица неисправностей которого фактически является преобразованной таблицей Кэли для операции умножения. *Мультипликативный источник неисправностей U_a^A с фиксированным аддитивным элементом a, $a \in A$, над кольцом A действует* на булеву функцию $f(\tilde{x}^n)$ следующим образом: источником U_a^A выбирается элемент $b \in A$, и вместо вычисления $f(\tilde{x}^n)$ происходит вычисление $f(\nu_A^{-1}((\nu_A(\tilde{x}^n) \cdot b) + a))$. Далее будем называть такой источник неисправностей *источником неисправностей над кольцом A с фиксированным элементом a*, при $a = 0$ — *источником неисправностей над кольцом A* (при этом индекс a опускается: U^A).

Следующие результаты второй главы касаются источников неисправностей над кольцами. Получены следующие оценки.

Теорема 5 (Антюфеев Г. В. [57])**.** *Пусть A — специальное кольцо, такое что $|A| = 2^n$. Тогда справедливо неравенство:*

$$\frac{2^n}{2} \leqslant L^{\mathrm{diagn}}(U^A, n).$$

Следствие 4 (Антюфеев Г. В. [57])**.** *Пусть A — специальное кольцо, такое что $|A| = 2^n$. Тогда функция Шеннона длины диагностического теста относительно источника неисправностей над кольцом A имеет следующий порядок роста:*

$$L^{\mathrm{diagn}}(U^A, n) = \Theta(2^n).$$

В теореме 6 описываются легкотестируемые функции относительно источников неисправностей $U_k^{\mathbb{Z}_{2^n}}$ над кольцом $\mathbb{Z}_{2^n}$ посредством установления

связи между существованием диагностических тестов минимально возможной длины и отделимостью по столбцам таблиц неисправностей.

Теорема 6 (Антюфеев Г. В. [57]). *Пусть $A = \mathbb{Z}_{2^n}$. И пусть на булеву функцию $f(\tilde{x}^n)$ действует источник неисправностей U_k^A. Таблица неисправностей, соответствующая U_k^A, отделима по столбцам для любого k только тогда, когда для каждого k справедливо равенство:*

$$L^{\mathrm{diagn}}(U_k^A, f(\tilde{x}^n)) = n.$$

Третья глава посвящена сдвигам аргументов функций. *Источник U^{shifts} сдвигов переменных* действует на булеву функцию $f(x_1, \ldots, x_n)$ следующим образом. Источником выбираются число $k \in \{1, \ldots, n\}$ и набор $\widetilde{\gamma} = (\gamma_1, \ldots, \gamma_n) \in E_2^n$, и вместо вычисления $f(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ происходит вычисление $f(\alpha_{k+1}, \ldots, \alpha_n, \gamma_{n-k+1}, \ldots, \gamma_n)$.

В следующих двух теоремах получены оценки для функции Шеннона длины проверяющего и диагностического тестов.

Теорема 7 (Антюфеев Г. В. [60, 63]). *Справедливо равенство:*

$$L^{\mathrm{detect}}(U^{\mathrm{shifts}}, n) = 2.$$

Теорема 8 (Антюфеев Г. В. [60, 63]). *Имеют место неравенства:*

$$c' \cdot 2^{n/2} - 1 \leqslant L^{\mathrm{diagn}}(U^{\mathrm{shifts}}, n) \leqslant c \cdot 2^{n/2},$$

где при n нечётном $c' = \sqrt{2}/2$ и $c = 2\sqrt{2}$, а при n чётном $c' = 1$ и $c = 3$.

Следствие 5 (Антюфеев Г. В. [60, 63]). *Функция Шеннона длины диагностического теста относительно сдвигов переменных имеет следующий порядок*

роста:

$$L^{\mathrm{diagn}}(U^{\mathrm{shifts}}, n) = \Theta(\sqrt{2^n}).$$

Далее рассматриваются источники неисправностей, получающиеся фиксацией одного из параметров источника сдвигов переменных.

Источник *сдвигов переменных на k позиций* U_k^{shifts} действует на булеву функцию $f(x_1, \ldots, x_n)$ следующим образом. Источником выбирается набор $\widetilde{\gamma} = (\gamma_1, \ldots, \gamma_k)$, и вместо вычисления $f(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ происходит вычисление $f(\alpha_{k+1}, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_k)$.

Для U_k^{shifts} установлено следующее утверждение.

Теорема 9 (Антюфеев Г. В. [60])**.** *Для k, n, таких что $1 \leqslant k \leqslant n$, имеют место неравенства:*

$$\min(2^k - 1, 2^{n-k}) \leqslant L^{\mathrm{diagn}}(U_k^{\mathrm{shifts}}, n) \leqslant \min(2^k, 2^{n-k} + 1).$$

Заметим, что теорема 9 определяет значение функции Шеннона с точностью до единицы.

Источник *сдвигов переменных с фиксированным замещающим набором* $\tilde{\gamma}$ обозначается следующим образом: $U_{\tilde{\gamma}}^{\mathrm{shifts}}$. Источником выбирается число $k = 1, \ldots, n$, и вместо вычисления $f(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ происходит вычисление $f(\alpha_{k+1}, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_k)$.

Для $U_{\tilde{\gamma}}^{\mathrm{shifts}}$ получены следующие оценки.

Теорема 10 (Антюфеев Г. В. [58])**.** *Для любого $\tilde{\gamma} \in E_2^n$ справедливо неравенство:*

$$\left\lceil \frac{n}{2} \right\rceil \leqslant L^{\mathrm{diagn}}(U_{\tilde{\gamma}}^{\mathrm{shifts}}, n).$$

Следствие 6 (Антюфеев Г. В. [58])**.** *Для любого $\tilde{\gamma} \in E_2^n$ функция Шеннона длины диагностического теста относительно сдвигов переменных с фикси-*

рованным замещающим набором имеет следующий порядок роста:

$$L^{\mathrm{diagn}}(U_{\tilde{\gamma}}^{\mathrm{shifts}}, n) = \Theta(n).$$

В теореме 11 описываются легкотестируемые функции относительно источников неисправностей $U_{\tilde{\gamma}}^{\mathrm{shifts}}$.

Теорема 11 (Антюфеев Г. В. [57, 61])**.** *Пусть $n > 1$ и на произвольную булеву функцию $f(\tilde{x}^n)$ действует источник неисправностей $U_{\tilde{\gamma}}^{shifts}$. Если таблица неисправностей, соответствующая $U_{\tilde{\gamma}}^{shifts}$, отделима по столбцам для любого $\tilde{\gamma}$, тогда для каждого $\tilde{\gamma}$ справедливо неравенство:*

$$L^{\mathrm{diagn}}(U_{\tilde{\gamma}}^{\mathrm{shifts}}, f(\tilde{x}^n)) \leqslant 2\log_2 \left\lfloor \frac{n}{2} \right\rfloor + 3.$$

Следствие 7 [57, 61]**.** *Пусть $n > 1$, и пусть на произвольную булеву функцию $f(\tilde{x}^n)$ действует источник неисправностей $U_{\tilde{\gamma}}^{shifts}$. Если таблица неисправностей, соответствующая $U_{\tilde{\gamma}}^{shifts}$, отделима по столбцам для любого $\tilde{\gamma}$, тогда для каждого $\tilde{\gamma}$ длина диагностического теста относительно сдвигов переменных с фиксированным замещающим набором имеет следующий порядок роста:*

$$L^{\mathrm{diagn}}(U_{\tilde{\gamma}}^{\mathrm{shifts}}, f(\tilde{x}^n)) = \Theta(\log n).$$

Степень достоверности

Достоверность полученных результатов обеспечивается строгими математическими выкладками и доказательствами, апробацией на конференциях и семинарах, а также публикациями в рецензируемых научных журналах.

Апробация результатов

Результаты исследований докладывались на следующих научных конференциях и семинарах:

- Конференция молодых специалистов «ОАО НИИ ВК имени М.А. Карцева» (Москва, 4 декабря 2012 г.);
- IX Международная конференция «Дискретные модели в теории управляющих систем» (Москва и Подмосковье, 20-22 мая 2015 г.);
- X Международная конференция «Дискретные модели в теории управляющих систем» (Москва и Подмосковье, 23-25 мая 2018 г.);
- XI Международная конференция «Дискретные модели в теории управляющих систем» (Москва и Подмосковье, 26-29 мая 2023 г.);
- XI Международный семинар «Дискретная математика и ее приложения», посвящённый 80-летию со дня рождения академика О. Б. Лупанова (Москва, 18–23 июня 2012 г.);
- семинар «Теория управляющих систем и математические модели СБИС», проводимый на кафедре математической кибернетики факультета вычислительной математики и кибернетики МГУ имени М. В. Ломоносова (Москва, 19 апреля 2013 г.);
- семинар «Дискретная математика и математическая кибернетика», проводимый на кафедре математической кибернетики факультета вычислительной математики и кибернетики МГУ имени М. В. Ломоносова (Москва, 23 мая 2014 г.);
- спецсеминар «Синтез управляющих систем», проводимый на кафедре дискретной математики механико-математического факультета МГУ имени М. В. Ломоносова (Москва, 24 марта 2022 г.);

- научно-исследовательский семинар «Математические вопросы кибернетики», проводимый совместно кафедрами дискретной математики и математической теории интеллектуальных систем механико-математического факультета МГУ имени М.В. Ломоносова и кафедрой математической кибернетики факультета вычислительной математики и кибернетики МГУ имени М. В. Ломоносова (Москва, 17 мая 2024 г.).

Глава 1

О тестах относительно константных неисправностей на входах схем

В настоящей главе приводятся результаты, касающиеся константного источника неисправностей. Исследуется как классический источник неисправностей, действие которого заключается в подстановке констант вместо любых аргументов функций, так и источник локальных константных неисправностей, который действует только на аргументы, идущие подряд в сигнатуре функции.

Напомним определения источников неисправностей, исследуемых в данной главе.

Источник U^{c} константных неисправностей действует на булеву функцию $f(x_1, x_2, \ldots, x_n)$ следующим образом. Источником выбираются переменные из списка $x_1, x_2, \ldots, x_n$, и вместо выбранных переменных производится подстановка констант из E_2.

Пусть $k \in \{1, \ldots, n\}$. Источник U_k^{lc} *локальных константных k-кратных неисправностей* действует на булеву функцию $f(x_1, \ldots, x_n)$ следующим образом. Источником выбирается двоичный набор $\widetilde{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_k) \in E_2^k$, где $k \leqslant n$, а также натуральное число m, $1 \leqslant m \leqslant n - k + 1$, и вместо вычисления $f(x_1, \ldots, x_m, \ldots, x_{m+k-1}, \ldots, x_n)$ происходит вычисление $f(x_1, \ldots, x_{m-1}, \varepsilon_1, \ldots, \varepsilon_k, x_{m+k}, \ldots, x_n)$.

§ 1.1. Оценки функций Шеннона длины диагностического теста относительно константных и локальных k-кратных константных неисправностей на входах схем

Получим нижнюю оценку функции Шеннона длины диагностического теста относительно локальных k-кратных константных неисправностей. Далее, используя эту оценку, выводится асимптотика логарифма исследуемой функции, а также нижняя оценка функции Шеннона длины диагностического теста относительно константных неисправностей. После чего получим порядок функции Шеннона длины диагностического теста относительно локальных k-кратных константных неисправностей.

Теорема 1 (Антюфеев Г. В. [60, 64])**.** *Для k, n, таких что $1 \leqslant k \leqslant n/2$, справедливо неравенство:*

$$L^{\mathrm{diagn}}\left(U_k^{\mathrm{lc}}, n\right) \geqslant \frac{2^{k+1}\left(n-k+1\right)-2}{\left(n-k+2\right)}.$$

Доказательство. Рассмотрим функцию

$$f\left(\widetilde{x}\right) = \bigvee_{(\sigma_1,\ldots,\sigma_k)\in E_2^k} x_1^{\sigma_1}\ldots x_k^{\sigma_k} x_{k+1}^{\sigma_{k+1}}\ldots x_n^{\sigma_n},$$

в которой для любого r, $r = k+1,\ldots,n$, выполнено равенство $\sigma_r = \sigma_{r'}$, где $r' \in \{1,\ldots,k\}$, и $r' \equiv r \pmod{k}$. Для всякого набора $\widetilde{\varepsilon} = (\varepsilon_1,\ldots,\varepsilon_k) \in E_2^k$ положим $\nu(\widetilde{\varepsilon}) = \sum_{i=1}^{k} \varepsilon_i 2^{k-i}$. Функции неисправности будем обозначать следующим образом:

$$f_{\nu(\widetilde{\varepsilon}),k,m}(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_{m-1}, \varepsilon_1, \ldots, \varepsilon_k, x_{m+k}, \ldots, x_n).$$

Упорядочим функции из множества $F_{U_k^k}$: f, $f_{0,k,1}$, $f_{1,k,1}$, $\ldots$, $f_{2^k-1,k,1}$, $f_{0,k,2}$, $f_{1,k,2}$,$\ldots$, $f_{2^k-1,k,2}$,$\ldots$, $f_{0,k,n-k+1}$, $f_{1,k,n-k+1}$,$\ldots$, $f_{2^k-1,k,n-k+1}$.

Столбцы значений этих функций, взятых в указанном порядке, образуют матрицу M_0, которая имеет размеры $2^n \times \left(2^k\,(n-k+1)+1\right)$. Матрица M_0 состоит из столбца значений функции f и из $s = n-k+1$ блоков столбцов по $t = 2^k$ столбцов в каждом блоке, причем столбцы одного блока соответствуют всем функциям вида $f_{i,k,m}$, у которых третьи индексы попарно равны.

В условиях теоремы для каждого двоичного набора $\widetilde{\varepsilon} = (\,\varepsilon_1, \ldots,\, \varepsilon_k)$ и для каждого m, $1 \leqslant m \leqslant n-k+1$, функция $f_{\nu(\widetilde{\varepsilon}),k,m}\ (x_1, x_2, \ldots, x_n)$ имеет вид:

$$f_{\nu(\widetilde{\varepsilon}),k,m}\ (x_1, x_2, \ldots, x_n) = x_1^{\delta_1} \ldots x_{m-1}^{\delta_{m-1}}\, x_{m+k}^{\delta_{m+k}}\ \ldots x_n^{\delta_n}.$$

Причем для любого r'', $r'' \in \{1, \ldots, m-1\} \cup \{m+k, \ldots, n\}$, выполнено равенство $\delta_{r''} = \varepsilon_{r'}$, где $r' \in \{1, \ldots, k\}$ и $r' \equiv r'' - m + 1 \pmod{k}$. Поэтому (так как $k < n$) в каждой строке матрицы M_0 в пределах любого одного блока имеется не более одной единицы.

Одинаковых столбцов в матрице M_0 нет. Действительно, предположение о наличии одинаковых столбцов в разных блоках противоречит тому, что соответствующие этим столбцам функции являются элементарными конъюнкциями различных множеств переменных. Предположение о наличии одинаковых столбцов в одном блоке противоречит тому, что в силу условия $k \leqslant n/2$ соответствующие этим столбцам функции являются элементарными конъюнкциями равных множеств переменных, но при этом наборы степеней переменных из этих конъюнкций различны.

Столбец значений исходной функции очевидным образом отличен от столбца значений любой из функций вида $f_{i,k,m}$.

Пусть в этой матрице M_0 выбрано l строк так, что все столбцы в составленной из этих строк таблице M' попарно различны (т. е. соответствующие этим l строкам наборы значений входных переменных образуют диагности-

ческий тест), а l – минимально возможное. Удалим в M' первый столбец и линейно переупорядочим оставшиеся в M' столбцы (не переставляя их) по неубыванию веса, т. е. числа единиц в столбце. Тогда, поскольку все столбцы разные, среди всех столбцов в первом (в соответствии с указанным линейным порядком) – не менее нуля единиц, в следующих l – не менее чем по одной единице в каждом, в остальных $ts-(l+1)$ – не менее чем по две единицы в каждом (иначе имелись бы равные столбцы). Значит, общее число единиц в таблице не менее чем $l+2(ts-l-1)$.

С другой стороны, так как число единиц в каждой строке меньше либо равно s, то общее число единиц в матрице меньше либо равно sl. Получаем неравенство: $sl \geqslant l+2\left(ts-l-1\right)$, т. е. $l \geqslant \frac{2ts-2}{s+1}$. Подставляя значения t и s, получаем: $L^{\text{diagn}}\left(U_k^{\text{lc}}, n\right) \geqslant L^{\text{diagn}}\left(U_k^{\text{lc}}, f\left(\widetilde{x}^n\right)\right) \geqslant \frac{2^{k+1}(n-k+1)-2}{n-k+2}$. Теорема доказана. □

Сформулируем в виде леммы очевидное утверждение, которое далее потребуется в нескольких местах.

Лемма 1. *Для любой булевой функции $f(x_1, x_2, \ldots, x_n)$ число попарно неравных функций во множестве $F_{U_k^{lc}}$ не превосходит $(n-k+1)\,2^k+1$.* □

Следствие 1 (Антюфеев Г. В. [60, 64])**.** *При $n \to \infty, k = k(n) \to \infty$, $1 \leqslant k \leqslant n/2, \log_2 n = o(k)$, справедливо асимптотическое равенство:*

$$\log_2 L^{\text{diagn}}(U_k^{\text{lc}}, n) = k(1+o(1)).$$

Доказательство. По теореме 1 имеет место неравенство:

$$\log_2 L^{\text{diagn}}\left(U_k^{\text{lc}}, n\right) \geqslant k(1+o\left(1\right)).$$

Из леммы 1 в условиях данной теоремы для любой булевой функции $f(x_1, x_2, \ldots, x_n)$ имеет место неравенство:

$$\log_2 L^{\text{diagn}}\left(U_k^{\text{lc}}, f\left(\widetilde{x}^n\right)\right) \leqslant \log_2\left((n-k+1)\,2^k\right) = k(1+o\,(1)),$$

откуда и вытекает требуемое. Следствие доказано. □

Заметим, что асимптотика логарифма функции Шеннона длины диагностического теста относительно локальных k-кратных константных неисправностей в условиях доказанного следствия не зависит от количества переменных n.

В статье [28] Носковым В. Н. установлены оценки

$$\frac{2^{n/2}}{2\sqrt{n}} \leqslant L^{\text{diagn}}\left(U^{\text{c}}, n\right) \leqslant 4\,(1+n)^3\,2^{0{,}773n}.$$

В той же статье [28, сноска на с. 74] Носков В. Н. справедливо отмечал, что можно доказать неравенство $L^{\text{diagn}}\left(U^{\text{c}}, n\right) \geqslant 2^{\left\lfloor \frac{n}{2} \right\rfloor} - 1$.

В работах [35, 36] Попков К. А. получил следующую оценку:

$$L^{diagn}(U^c, n) \geqslant \begin{cases} 2^{n/2}, & \text{если } n \text{ чётно}, \\ \left\lfloor \frac{2\sqrt{2}}{3} \cdot 2^{n/2} \right\rfloor, & \text{если } n \text{ нечётно}. \end{cases}$$

Полагая $k = \left\lfloor \frac{n}{2} \right\rfloor$, получим из теоремы 1 чуть более сильную нижнюю оценку:

$$L^{\text{diagn}}\left(U^{\text{c}}, n\right) \geqslant L^{\text{diagn}}\left(U^{\text{lc}}_{\lfloor n/2 \rfloor}, n\right) \geqslant \\ \geqslant \frac{2^{\left\lfloor \frac{n}{2} \right\rfloor + 1}\left(\left\lceil \frac{n}{2} \right\rceil + 1\right) - 2}{\left(\left\lceil \frac{n}{2} \right\rceil + 2\right)} \geqslant 2 \cdot 2^{\left\lfloor \frac{n}{2} \right\rfloor} \cdot (1 + o\,(1))$$

при условии стремления n к бесконечности. Значит, имеет место следующая теорема:

Теорема 2 (Антюфеев Г. В. [60, 64])**.** *При $n \to \infty$ справедливо асимптотическое неравенство:*

$$L^{\mathrm{diagn}}(U^{\mathrm{c}}, n) \geqslant 2 \cdot 2^{\left\lfloor \frac{n}{2} \right\rfloor}(1 + o(1)).$$

□

Получим порядок функции Шеннона длины диагностического теста относительно локальных константных неисправностей при некоторых ограничениях на k в зависимости от n.

Теорема 3 (Антюфеев Г. В. [59])**.** *Пусть n и k — целые положительные, $c > 1$ — действительная константа, $2 \leqslant k \leqslant \frac{n}{2c}$. Тогда имеют место неравенства:*

$$(n - 2k + 3 - \lceil \log_2(n - k + 1) \rceil) \cdot 2^{k-2} - 1 \leqslant L^{\mathrm{diagn}}(U_k^{\mathrm{lc}}, n) \leqslant (n - k + 1) \cdot 2^k.$$

Доказательство. Верхняя оценка функции Шеннона длины диагностического теста следует из леммы 1.

Докажем нижнюю оценку функции Шеннона. Оценим такое минимальное натуральное l, при котором имеет место неравенство $(n-l-k+1) \cdot 2^{k-2} \leqslant 2^l$. Покажем, что верна оценка $k-2+\lceil \log_2(n-k+1) \rceil \geqslant l$:

$$1 - \lceil \log_2(n - k + 1) \rceil \leqslant n,$$
$$(n - 2k + 3 - \lceil \log_2(n - k + 1) \rceil) \cdot 2^{k-2} \leqslant (n - k + 1) \cdot 2^{k-1},$$
$$(n - (k - 2 + \lceil \log_2(n - k + 1) \rceil) - k + 1) \cdot 2^{k-2} \leqslant 2^{k-2+\lceil \log_2(n-k+1) \rceil}.$$

Выберем некоторое инъективное отображение $\eta : \{1, \ldots, n-l-k+1\} \times E_2^{k-2} \to E_2^l$ (оно, очевидно, существует). Рассмотрим булеву функцию $h_{n,k}(\tilde{x}^n)$, которая

равна:

$$\bigvee_{j=1}^{n-l-k+1} \bigvee_{(\sigma_2,\ldots,\sigma_{k-1})\in E_2^{k-2}} \bar{x}_1\cdots\bar{x}_{j-1}x_j x_{j+1}^{\sigma_2}\cdots x_{j+k-2}^{\sigma_{k-1}}x_{j+k-1}\bar{x}_{j+k}\cdots\bar{x}_{n-l}x_{n-l+1}^{\xi_{j,1}}\cdots x_n^{\xi_{j,l}},$$

где $(\xi_{j,1},\ldots,\xi_{j,l}) = \eta(j,(\sigma_2,\ldots,\sigma_{k-1}))$. Для всякого j, $j \in \{1,\ldots,n-l-k+1\}$, при подстановке в функцию $h_{n,k}(x_1,\ldots,x_n)$ булевых констант $1,\sigma_2,\ldots,\sigma_{k-1},1$ вместо переменных $x_j, x_{j+1},\ldots,x_{j+k-1}$ (соответственно) получается функция неисправности вида:

$$h_{n,k}^{(j,(\sigma_2,\ldots,\sigma_{k-1}))}(\tilde{x}^n) = \bar{x}_1\cdots\bar{x}_{j-1}\bar{x}_{j+k}\cdots\bar{x}_{n-l}x_{n-l+1}^{\xi_{j,1}}\cdots x_n^{\xi_{j,l}},$$

где $(\xi_{j,1},\ldots,\xi_{j,l}) = \eta(j,(\sigma_2,\ldots,\sigma_{k-1}))$.

Пусть $h_{n,k}^{(j',(\sigma'_2,\ldots,\sigma'_{k-1}))}(\tilde{x}^n)$ и $h_{n,k}^{(j'',(\sigma''_2,\ldots,\sigma''_{k-1}))}(\tilde{x}^n)$ — две различные функции неисправности, $(j',(\sigma'_2,\ldots,\sigma'_{k-1})) \neq (j'',(\sigma''_2,\ldots,\sigma''_{k-1}))$. Поскольку любые две такие функции обращаются в единицу на непересекающихся множествах наборов в силу инъективности отображения η, заключаем: для того чтобы попарно отличить друг от друга все различные функции неисправности, требуется не менее $(n-l-k+1)\cdot 2^{k-2}-1$ наборов. Отсюда получаем оценку:

$$L^{\mathrm{dg}}(U_k^{\mathrm{lc}},n) \geqslant L^{\mathrm{dg}}(U_k^{\mathrm{lc}},h_{n,k}) \geqslant (n-2k+3-\lceil\log_2(n-k+1)\rceil)\cdot 2^{k-2}-1.$$

Теорема доказана. □

Следствие 8 (Антюфеев Г. В. [59])**.** *Пусть n и k — целые положительные, $c > 1$ — действительная константа, $n \to \infty$, $2 \leqslant k \leqslant \frac{n}{2c}$, $k = k(n)$. Функция Шеннона длины диагностического теста относительно локальных*

k-кратных константных неисправностей имеет следующий порядок роста:

$$L^{\mathrm{diagn}}(U_k^{\mathrm{lc}}, n) = \Theta(n2^k).$$

□

§ 1.2. Оценки функций Шеннона длины проверяющего теста относительно локальных k-кратных константных неисправностей на входах схем

Получим оценки функции Шеннона длины проверяющего теста относительно k-кратных локальных константных неисправностей.

Теорема 4 (Антюфеев Г. В. [59]). *Пусть n и k — целые положительные, $2 \leqslant k \leqslant n$. Тогда имеют место неравенства:*

$$2 \cdot \left(\left\lfloor \frac{2 \cdot \left(n - \left\lceil \log_2 \left\lfloor \frac{2n}{k+1} \right\rfloor \right\rceil \right)}{k+1} \right\rfloor - 2 \right) \leqslant L^{\mathrm{detect}}(U_k^{\mathrm{lc}}, n) \leqslant 4 \cdot \left\lceil \frac{n+2}{k+1} \right\rceil - 4.$$

Доказательство. Установим справедливость верхней оценки $L^{\mathrm{detect}}(U_k^{\mathrm{lc}}, n)$. Рассмотрим произвольную булеву функцию $f(\tilde{x}^n)$. Организуем следующий процесс, выбирающий по функции $f(\tilde{x}^n)$ конечную возрастающую последовательность A_f натуральных чисел ν_1, $\nu_2, \ldots,$ ν_t, являющихся индексами существенных переменных функции f.

Если функция $f(\tilde{x}^n)$ тождественно равна константе, то искомая последовательность A_f не содержит элементов.

Далее рассматривается альтернативный случай. Разобьем набор $(x_1, \ldots, x_n)$ всех переменных на непересекающиеся последовательные отрезки: $d_1, d_2, d_3, \ldots, d_{w-1}, d_w$.

При этом в отрезке d_1 ровно k или $k-1$ переменных, в каждом из отрезков $d_2, \ldots, d_{w-1}$ ровно по $k+1$ переменных, в отрезке d_w — не более чем k переменных и не менее чем одна. Нетрудно видеть, что при $n = k$ имеется ровно один отрезок, а при $n > k$ число отрезков $w = \left\lceil \frac{n+2}{k+1} \right\rceil$.

Элементами последовательности A_f оказываются (при наличии существенных переменных функции f в соответствующих отрезках): максимальный индекс существенной переменной из отрезка d_1, минимальный и максимальный индексы существенных переменных из отрезка d_j ($j \in \{2, \ldots, w-1\}$; если в d_j имеется ровно одна существенная переменная, то ее индекс используется один раз в качестве элемента последовательности A_f), минимальный индекс существенной переменной из отрезка d_w. Другие числа не могут являться элементами A_f, выбранные же элементы ν_1, $\nu_2, \ldots$, ν_t упорядочиваются по возрастанию. Очевидно, что $t = |A_f| \leqslant 2w - 2 \leqslant 2 \cdot \left\lceil \frac{n+2}{k+1} \right\rceil - 2$.

Для каждого элемента ν_s построенной последовательности ($s \in \{1, \ldots, t\}$) включим в множество T два соседних по переменной x_{ν_s} набора значений переменных $(x_1, \ldots, x_n)$, на которых функция f принимает разные значения (такая пара наборов найдется в силу существенности переменной x_{ν_s} для функции f). Один и тот же набор из множества T в указанном в предыдущем предложении смысле может входить в несколько пар наборов — для нескольких существенных переменных функции f. Ясно, что при этом $|T| \leqslant 4 \cdot \left\lceil \frac{n+2}{k+1} \right\rceil - 4$.

Оказывается, T — проверяющий тест для функции f относительно локальных константных неисправностей кратности k на входах схем. Действительно, рассмотрим подстановку k произвольных булевых констант σ_1, $\sigma_2, \ldots$, σ_k вместо переменных x_j, $x_{j+1}, \ldots$, x_{j+k-1} соответственно ($j \in \{1, \ldots, n-k+1\}$).

Если все эти переменные функции $f(\tilde{x}^n)$ — фиктивные, то соответствующая подстановке функция неисправности $g(\tilde{x}^n)$ неотличима от $f(\tilde{x}^n)$.

Если же среди переменных x_j, $x_{j+1}, \ldots, x_{j+k-1}$ имеется хотя бы одна существенная переменная, то среди индексов этих переменных по построению последовательности A_f найдется хотя бы один элемент $\nu_{s'}$ этой последовательности.

Действительно, если все переменные x_j, $x_{j+1}, \ldots, x_{j+k-1}$ попадают в один отрезок, то в случае отрезка d_1 или d_w переменные x_j, $x_{j+1}, \ldots, x_{j+k-1}$ исчерпывают все переменные отрезка, так что искомый элемент $\nu_{s'}$ найдется (ибо не все переменные фиктивны для f), а в случае любого отрезка из числа $d_2, \ldots, d_{w-1}$ переменными x_j, $x_{j+1}, \ldots, x_{j+k-1}$ выпускается ровно одна переменная из отрезка, но поскольку среди переменных x_j, $x_{j+1}, \ldots, x_{j+k-1}$ есть существенная, то среди них есть переменная с минимальным или с максимальным индексом существенной переменной из отрезка, так что искомый элемент $\nu_{s'}$ найдется.

Иначе если переменные x_j, $x_{j+1}, \ldots, x_{j+k-1}$ попадают в два последовательных отрезка, то в силу наличия среди них существенной переменной по построению последовательности A_f среди этих переменных найдется переменная с максимальным индексом $\nu_{s'}$ из первого (по возрастанию индексов) отрезка или найдется переменная с минимальным индексом $\nu_{s'}$ из второго отрезка. Значит, во всех возможных случаях искомый элемент $\nu_{s'}$ существует.

На двух соответствующих элементу $\nu_{s'}$ соседних наборах из T функция f отличается от соответствующей рассматриваемой подстановке функции неисправности $g(\tilde{x}^n)$, так как, в отличие от f, функция g на этих наборах принимает одинаковые значения. Отметим, что в случае не содержащей элементов последовательности A_f функция f тождественно равна константе, так что минимальный проверяющий тест для f пуст. Верхняя оценка доказана.

Докажем нижнюю оценку. Пусть сначала $n > k$. Оценим такое минимальное натуральное l, при котором имеет место неравенство $\left\lfloor \frac{2(n-l)}{k+1} \right\rfloor \leqslant 2^l$. Покажем, что верна оценка $l \leqslant \left\lceil \log_2 \left\lfloor \frac{2n}{k+1} \right\rfloor \right\rceil$:

$$2\left(n - \left\lceil \log_2 \left\lfloor \frac{2n}{k+1} \right\rfloor \right\rceil\right) \leqslant 2n,$$

$$\left\lfloor \frac{2\left(n - \left\lceil \log_2 \left\lfloor \frac{2n}{k+1} \right\rfloor \right\rceil\right)}{k+1} \right\rfloor \leqslant \left\lfloor \frac{2n}{k+1} \right\rfloor,$$

$$\left\lfloor \frac{2\left(n - \left\lceil \log_2 \left\lfloor \frac{2n}{k+1} \right\rfloor \right\rceil\right)}{k+1} \right\rfloor \leqslant 2^{\left\lceil \log_2 \left\lfloor \frac{2n}{k+1} \right\rfloor \right\rceil}.$$

Рассмотрим булеву функцию мультиплексорного типа:

$$h_{n,k}(x_1, \ldots, x_{n-l}, x_{n-l+1}, \ldots, x_n) = \bigvee_{j=0}^{\left\lfloor \frac{2(n-l)}{k+1} \right\rfloor - 1} K_j(x_{n-l+1}, \ldots, x_n) \cdot x_{\left\lfloor \frac{j(k+1)}{2} \right\rfloor + 1},$$

где $K_j(x_{n-l+1}, \ldots, x_n) = x_{n-l+1}^{\delta_1} \cdots x_n^{\delta_l}$, причем $(\delta_1, \ldots, \delta_l) \in E_2^l$ и $\sum\limits_{i=1}^{l} \delta_i \cdot 2^{l-i} = j$. Неисправность, связанная с тем, что вместо k подряд идущих переменных $x_{\left\lfloor \frac{j(k+1)}{2} \right\rfloor + 2}, \ldots, x_{\left\lfloor \frac{(j+2)(k+1)}{2} \right\rfloor}$ подставляются булевы константы так, что на место переменной $x_{\left\lfloor \frac{(j+1)(k+1)}{2} \right\rfloor + 1}$ подставлена константа σ ($j \in \{0, \ldots, \left\lfloor \frac{2(n-l)}{k+1} \right\rfloor - 2\}$, $\sigma \in E_2$), обнаруживается на тех и только тех наборах значений переменных $(x_1, \ldots, x_n)$, на которых $x_{\left\lfloor \frac{(j+1)(k+1)}{2} \right\rfloor + 1} = \bar{\sigma}$, $x_{n-l+i} = \delta_i'$ ($i = 1, 2, \ldots, l$), причем $\sum\limits_{i=1}^{l} \delta_i' \cdot 2^{l-i} = j + 1$. А поскольку эти множества наборов для различных пар $(\sigma, (\delta_1', \ldots, \delta_l'))$ попарно не пересекаются, из каждого из них в любой проверяющий тест должен войти хотя бы один

набор, откуда получаем нижнюю оценку:

$$L^{\mathrm{detect}}(U_k^{\mathrm{lc}}, n) \geqslant L^{\mathrm{detect}}(U_k^{\mathrm{lc}}, h_{n,k}) \geqslant$$
$$2 \cdot \left(\left\lfloor \frac{2(n-l)}{k+1} \right\rfloor - 2 \right) \geqslant 2 \cdot \left(\left\lfloor \frac{2 \cdot \left(n - \left\lceil \log_2 \left\lfloor \frac{2n}{k+1} \right\rfloor \right\rceil \right)}{k+1} \right\rfloor - 2 \right).$$

При $n = k$ имеем: $L^{\mathrm{detect}}(U_k^{\mathrm{lc}}, k) \geqslant L^{\mathrm{detect}}(U_k^{\mathrm{lc}}, x_1) \geqslant 2$, что лучше нижней оценки, заявленной в формулировке теоремы. Теорема доказана. □

Используя доказанную теорему, получим асимптотику для функции Шеннона длины проверяющего теста относительно локальных k-кратных константных неисправностей.

Следствие 9 (Антюфеев Г. В. [59])**.** *Пусть n и k — целые положительные, $n \to \infty$, $2 \leqslant k \leqslant n$, $k = k(n)$, $k = o(n)$. Тогда имеет место асимптотическое равенство:*

$$L^{\mathrm{detect}}(U_k^{\mathrm{lc}}, n) = \frac{4n}{k+1} \cdot (1 + o(1)).$$

□

Глава 2

О тестах относительно источников неисправностей над кольцами

В данной главе вводится понятие тестов над кольцами. Фактически основное отличие от определённых ранее терминов заключается в том, что рассматриваются не булевы функции, а их обобщения до двоичных функций, областью определения которых являются элементы кольца.

§ 2.1. Определения и обозначения

Напомним основные определения.

Коммутативное кольцо A — множество с двумя бинарными операциями (сложение и умножение), которое удовлетворяет следующим аксиомам:

1. По сложению A является абелевой группой.
2. Умножение ассоциативно: $(xy)z = x(yz)$ и дистрибутивно относительно сложения: $x(y+z) = xy + xz,\ (y+z)x = yx + xz$.
3. Для всех x, $y \in A$ выполняется $xy = yx$.
4. Существует такой элемент $1 \in A$, что $x1 = 1x = x$ для всех $x \in A$. Элемент 1 называется *единицей кольца* A *или единичным элементом кольца* A.

Конечное кольцо — кольцо, множество которого конечно. В диссертации термин *кольцо* будет означать конечное коммутативное кольцо. *Таблица Кэли для операции умножения кольца* A (далее просто *таблица Кэли*) — таблица, строки и столбцы которой индексированы элементами кольца A, а в каждой клетке записан результат применения операции умножения кольца A к элементам, соответствующим строке и столбцу.

Порядок кольца — количество элементов кольца. Порядок кольца A обозначается $|A|$.

Пусть $B, C \subset A$, тогда $B + C \subset A$ и состоит из всех элементов $b + c$, а $BC \subset A$ и состоит из всех элементов bc, $b \in B, c \in C$. При сложении или умножении с одноэлементным подмножеством $\{x\}$ фигурные скобки иногда могут опускаться.

Идеал I в кольце A — аддитивная подгруппа со свойством $AI \subset I$. Пусть $x \in A$, тогда все кратные xa некоторого элемента $a \in A$ образуют идеал, который обозначается (a) и называется *главным*. *Кольцо главных идеалов* — кольцо, каждый идеал которого главный.

Произведение главных идеалов (a) и (b) — это идеал (ab), то есть $(a) \cdot (b) = (ab)$ (см., например, [4, с. 426]). Степень $(a)^n$ главного идеала (a) определяется так: $(a)^1 = (a), (a)^{n+1} = (a) \cdot (a)^n$, где $n \in \mathbb{N}$. Положим $(a)^0 = (a^0) = (1) = A$.

Нулевой идеал (0) может обозначаться 0. *Простой идеал* — такой идеал I кольца A, что $I \neq A$ и из $cb \in I$ следует $b \in I$ или $c \in I$. *Максимальный идеал* кольца A — всякий собственный идеал кольца, не содержащийся ни в каком другом собственном идеале.

Специальное кольцо — кольцо главных идеалов, имеющее только один простой идеал $I \neq A$ и $I^{n'} = (0)$ для некоторого $n' \in \mathbb{N}$.

Элемент a кольца A называется *обратимым*, если существует такой элемент b, $b \in A$, что $ab = ba = 1$, где 1 — единица кольца A. Если элемента b не существует, то элемент a кольца A называется *необратимым*.

Пусть $B \subset A$, тогда M^B — матрица, получающаяся из таблицы Кэли вычёркиванием столбцов, индексированных элементами из множества $A \setminus B$. Если $A = B$, то M^A — таблица Кэли.

В обозначении M^B намеренно опускается дополнительный индекс A, который позволил бы однозначно строить матрицу по обозначению. Это сделано для того, чтобы не загромождать обозначение. Здесь это не приводит к противоречиям. В обозначениях других типов матриц, получающихся из таблиц Кэли кольца A, индекс A также будет опущен.

Пусть $h : A \to A'$ — сюръективное отображение множества элементов кольца A на его подмножество A', $A' \subset A, A' \neq \varnothing$. То есть $h(a) = a'$ для $a \in A, a' \in A'$. Если $|A'| = 1$ и $b \in A'$, то используется обозначение $h \equiv b$.

Матрица M_h^B — матрица, получающаяся из матрицы M^B путём замены каждого элемента x каждого столбца M^B, индексированного элементом $y \in B$, на элемент $x + h(y), B \subset A$. Если $h \equiv a, a \in A$, то будем использовать обозначение M_a^B. Если $h \equiv 0, 0 \in A$, то будем использовать обозначение M^B.

Пусть $f^A(x)$ — двоичная функция, определённая на элементах кольца A. То есть $f^A : A \to E_2$. *Функция* $f^A(x)$ *обладает свойством* Ψ^I, где I — идеал кольца A, $I \neq (0)$, если для любого $\mathfrak{K} \in A/I$ существуют такие элементы $c \in \mathfrak{K}$ и $b \in \mathfrak{K}$, что $f^A(c) \neq f^A(b)$, где A/I — факторкольцо (см., например, [4, с. 64-68]). *Характеристическое множество* N_{f^A} функции $f^A(x)$ — множество всех элементов кольца A, на которых функция $f^A(x)$ равна 1.

Двоичная *матрица* M_{h,f^A}^B *таблицы Кэли* — матрица, получающаяся из таблицы Кэли путём замены каждого элемента матрицы M_h^B на значение

функции f^A от этого элемента, где $B \subset A$. Индекс A иногда опускается: $M^B_{h,f}$.

Во всех матрицах, получающихся из таблицы Кэли кольца A, индексация элементами из кольца A сохраняется. Столбец, индексированный элементом $a \in A$, будем называть столбцом a. Строку, индексированную элементом $a \in A$, будем называть строкой a.

Матрица M *отделима (по столбцам)*, если все её столбцы попарно различны.

Диагностический тест T над кольцом A относительно функции f^A — подмножество элементов кольца A такое, что для любых двух элементов a и b кольца A таких, что соответствующие им столбцы a и b матрицы $M^A_{0,f}$ не равны, существует такой элемент $t, t \in T$, что $f^A(ta + 0) \neq f^A(tb + 0)$. В таком случае будем говорить, что элемент t (или строка t, см. определение выше) *отличает* элементы a и b (или столбцы a и b, см. определение выше).

Длина теста T — количество элементов в этом тесте. Длина теста T обозначается $|T|$. Тест минимальной длины называется *минимальным*. Длина минимального диагностического теста на кольце A относительно функции f^A обозначается $L^{\text{diagn}}(A, f)$.

Пусть $|A| = m$. Обозначим через F^A — множество всех двоичных функций, определённых на элементах кольца A. Введём функцию шенноновского типа для длины диагностического теста на кольце A (относительно отображения $h \equiv 0$):

$$L^{\text{diagn}}(A, m) = \max_{f \in F^A} L^{\text{diagn}}(A, f).$$

Пусть выбрано кольцо A, такое что $|A| = 2^n$, и задана биекция $\nu_A : E_2^n \to A$. Обратное отображение к ν_A — это отображение $\nu_A^{-1} : A \to E_2^n$, такое что $\nu_A(\nu_A^{-1}(a)) = a$ для всех $a \in A$, и $\nu_A^{-1}(\nu_A(\tilde{\alpha}^n)) = \tilde{\alpha}^n$ для всех $\tilde{\alpha}^n \in E_2^n$. Введём источник неисправностей, таблица неисправностей которого фактически является преобразованной таблицей Кэли для операции

умножения. *Мультипликативный источник неисправностей U_a^A с фиксированным аддитивным элементом a, $a \in A$, над кольцом A действует* на булеву функцию $f(\tilde{x}^n)$ следующим образом: источником U_a^A выбирается элемент $b \in A$, и вместо вычисления $f(\tilde{x}^n)$ происходит вычисление $f(\nu_A^{-1}((\nu_A(\tilde{x}^n) \cdot b) + a))$. Далее будем называть такой источник неисправностей *источником неисправностей над кольцом A с фиксированным элементом a*, при $a = 0$ — *источником неисправностей над кольцом A* (при этом индекс a опускается: U^A).

§ 2.2. Оценка функции Шеннона длины диагностического теста и легкотестируемые функции относительно источников неисправностей над кольцами

Лемма 2. *Пусть A — специальное кольцо, такое что $|A| = n$. Тогда справедливо неравенство:*

$$\frac{n}{2} \leqslant L^{\mathrm{diagn}}(A, n).$$

Доказательство. Специальные кольца по определению имеют только один простой идеал P, и он всегда максимален [11, с. 282]. Следовательно, остальные идеалы являются его подидеалами.

Идеал P по определению является аддитивной подгруппой, и так как он максимален, то по определению он собственный. Из этого следует, что максимально возможное количество элементов в нём $\frac{n}{2}$, так как порядок подгруппы делит порядок группы (теорема Лагранжа, см., например, [10, с. 31]). Так как идеал P состоит из всех необратимых элементов (см., например, [1, с. 13]), то $A \setminus P$ состоит из всех обратимых элементов кольца, которые образуют группу по умножению. Обозначим её $E(A)$. Очевидно, $|E(A)| \geqslant \frac{n}{2}$.

Рассмотрим функцию f^A такую, что $N_{f^A} = \{a\}$ для некоторого $a \in E(A)$. Так как $E(A)$ — группа по умножению, то, чтобы отличить все

пары элементов в $E(A)$, потребуется $|E(A)| - 1$ элементов. И ещё один элемент — чтобы отличить элементы $|E(A)|$ от элементов P, функция f^A на которых равна нулю. Таким образом, получается нижняя оценка $\frac{n}{2}$. Лемма доказана. □

Из леммы 2 следует теорема 5.

Теорема 5 (Антюфеев Г. В. [57]). *Пусть A — специальное кольцо, такое что $|A| = 2^n$. Тогда справедливо неравенство:*

$$\frac{2^n}{2} \leqslant L^{\text{diagn}}(U^A, n).$$

□

Из теоремы 5 получается следствие 4.

Следствие 4 (Антюфеев Г. В. [57]). *Пусть A — специальное кольцо, такое что $|A| = 2^n$. Тогда функция Шеннона длины диагностического теста относительно источника неисправностей над кольцом A имеет следующий порядок роста:*

$$L^{\text{diagn}}(U^A, n) = \Theta(2^n).$$

Доказательство. Верхняя оценка тривиальна. Так как $|A| = 2^n$, то, чтобы отличить столбцы матрицы $M^A_{0,f}$ относительно любой функции f, достаточно $2^n - 1$ элементов. Следовательно, $L^{diagn}(A, n) \leqslant 2^n - 1$. *Нижняя оценка* следует из теоремы 5. Следствие доказано. □

Рассмотрим теперь, как строить легкотестируемые функции относительно источников неисправностей над специальными кольцами. В качестве вспомогательного утверждения доказывается лемма 3, которая также будет использована в третьей главе для доказательства теоремы о легкотестируемых функциях относительно других источников неисправностей.

Лемма 3. *Пусть A — специальное кольцо и пусть $h : A \to A'$ — сюръективное отображение множества элементов кольца A на его подмножество A', $A' \subset A, A' \neq \varnothing$. Пусть, далее, в A имеется цепь главных идеалов:*

$$A \supsetneq (a) \supsetneq (a)^2 \supsetneq \cdots \supsetneq (a)^{l-1} \supsetneq (a)^l = (0), a \in A, l \in \mathbb{N}.$$

Зафиксируем $k \in \mathbb{N}$ такое, что $1 \leqslant k < l$. На элементах A задана функция f^A, обладающая свойством $\Psi^{(a)^k}$. Положим $B = \{a^i, a^{i+(l-k)}, a^{i+2(l-k)}, \ldots, a^{i+s(l-k)}\}$, где $i + s(l-k) \leqslant k$, $i \in \mathbb{N}_0$. Тогда в M^B_{h,f^A} существуют строки каждого вида $\tilde{\alpha}^{|B|} \in E_2^{|B|}$.

Доказательство. Длина цепи главных идеалов равна $l + 1$ (учитывается и само кольцо A), а $l - k$ — это длина «шага», с которым возможно строить требуемые строки в такой цепи.

Заметим, что $\left\lceil \frac{l+1}{l-k} \right\rceil - 2 \leqslant |B| \leqslant \left\lceil \frac{l+1}{l-k} \right\rceil - 1$. В данных неравенствах верхняя оценка не равна нижней, так как в зависимости от i искомые строки могут строиться, начиная с разных столбцов.

Зафиксируем произвольную строку $\tilde{\beta}^{|B|} \in E_2^{|B|}$. Обозначим $v = i + s(l-k)$, $v_m = v - (m-1)(l-k)$ и $B^m = \{a^{v_m}, \ldots, a^{v_1}\}$, где $m = 1, \ldots, s+1$. Докажем индукцией по m, что в $M^{B^m}_{h,f^A}$ существуют строки каждого вида $\tilde{\alpha}^m = (\beta_{s-m+1}, \ldots, \beta_s) \in E_2^{|B^m|}$.

База индукции. При $m = 1$ рассматривается матрица (столбец) $M^{\{a^{v_1}\}}_{h,f^A}$. Ей соответствует матрица $M^{\{a^{v_1}\}}$, элементы которой принадлежат идеалу $(a)^v$. Так как $v \leqslant k$, то по условию леммы $(a)^v \supset (a)^k$. Так как по условию леммы f^A обладает свойством $\Psi^{(a)^k}$, то, по определению матрицы $M^{\{a^{v_1}\}}_h$ и класса вычетов по идеалу $(a)^k$ (см., например, [4, с. 66]) получаем, что в $M^{\{a^{v_1}\}}_h$ имеются элементы $b \in A$ и $c \in A$, принадлежащие классу вычетов $h(a^v) + (a)^k$ по идеалу $(a)^k$, и такие, что $f^A(c) \neq f^A(b)$. Следовательно, в $M^{\{(a)^{v_1}\}}_{h,f^A}$ существуют строки каждого вида $\tilde{\alpha}^1 = (\beta_s) \in E_2^{|B^1|}$.

Индуктивный переход. Положим $d = h(a^{v_{m-1}})$, $d \in A$ и $e = h(a^{v_m}), e \in A$. Предположим по индукции, что в $M_{h,f^A}^{B^{m-1}}$ существуют строки каждого вида $\tilde{\alpha}^{m-1} = (\beta_{s-m+2}, \ldots, \beta_s) \in E_2^{|B^{m-1}|}$. Следовательно, для каких-то элементов $t, y \in A$ выполняется $f^A(t \cdot a^{v_{m-1}} + d) = f^A(y + d) = \beta_{s-m+2}$, где $y = t \cdot a^{v_{m-1}}$.

Рассмотрим теперь матрицу $M_{h,f^A}^{B^m}$ как расширенную матрицу, полученную из $M_{h,f^A}^{B^{m-1}}$ приписыванием слева столбца a^{v_m}. Положим $x = t \cdot a^{v_m}$, $x \in A$, и пусть $\mathfrak{F} \in (a)^{v_m}/(a)^k$ такой, что $x \in \mathfrak{F}$. Так как $\mathfrak{F} = \{r\} + (a)^k$, для некоторого $r \in (a)^{v_m}$, и $A \supsetneq (a)^{v_m}$, то $\mathfrak{F} \in A/(a)^k$. Далее, по определениям, $x + e \in \mathfrak{F} + e \in A/(a)^k$. И, следовательно, по условию леммы существует элемент $z \in \mathfrak{F} + e$ такой, что $f^A(z) \neq f^A(x + e)$. Далее, можно показать (см., например, [10, с. 98]), что $z - e$ и x принадлежат одному классу вычетов по $(a)^k$. Из определений матриц следует, что элемент $z - e$ есть в столбце a^{v_m} матрицы M^{B^m}. Следовательно, существует элемент $t' \in A$, такой что $t' \cdot a^{v_m} = z - e$. Из этого и того, что $z - e$ и x принадлежат одному классу вычетов по $(a)^k$, следует, что существуют элементы $t'', t''', w \in A$ такие, что $x = t \cdot a^{v_m} = t'' \cdot a^k + w$ и $t' \cdot a^{v_m} = t''' \cdot a^k + w$. Учитывая это и то, что $t \cdot a^{v_{m-1}} = t \cdot a^{v_m} \cdot a^{l-k}$, получаем: $y = (t'' \cdot a^k + w) \cdot a^{l-k} = w \cdot a^{l-k}$ и $f^A(w \cdot a^{l-k} + d) = \beta_{s-m+2}$. Аналогично получаем, что $t' \cdot a^{v_{m-1}} = w \cdot a^{l-k}$ и, очевидно, $f^A(t' \cdot a^{v_{m-1}} + d) = \beta_{s-m+2}$.

Таким образом, в зависимости от β_{s-m+1} выбирается строка t' или t. Так как каждый столбец матрицы M^{B^m} получается из предыдущего умножением на $a^{(l-k)}$, то суффиксы $(\beta_{s-m+3}, \ldots, \beta_s)$ строк t и t' равны. Лемма доказана. □

Далее описывается класс легкотестируемых функций относительно источников неисправностей над некоторыми специальными кольцами с фиксированными элементами, которые состоят из 2^n элементов ($n \in \mathbb{N}$). В следующей главе аналогичным образом будет сформулирована теорема 11, в которой

будут описаны легкотестируемые функции при сдвигах аргументов. Однако оценка в теореме 11 будет отлична от оценки в теореме 6.

Теорема 6 (Антюфеев Г. В. [57])**.** *Пусть $A = \mathbb{Z}_{2^n}$. И пусть на булеву функцию $f(\tilde{x}^n)$ действует источник неисправностей U_k^A. Таблица неисправностей, соответствующая U_k^A, отделима по столбцам для любого k только тогда, когда для каждого k справедливо равенство:*

$$L^{\mathrm{diagn}}(U_k^A, f(\tilde{x}^n)) = n.$$

Доказательство. Положим $p = 2$. Для того чтобы при любом $k \in A$ матрица $M_{k,f}^A$ была отделима по столбцам, необходимо, чтобы функция f обладала свойством $\Psi^{(p)^{n-1}}$. Докажем необходимость этого. Рассмотрим столбцы p^{n-1} и p^n матрицы M_k^A. Столбец p^n состоит из одного элемента $p^n A + k$ кольца A. Так как $(p)^{n-1} \supsetneq (p)^n = (0)$, то столбец $(p)^{n-1}$ состоит из элементов $p^{n-1}A + k$ и $p^n A + k$. Значит, чтобы столбцы p^{n-1} и p^n матрицы $M_{k,f}^A$ были различны, необходимо, чтобы $f(p^{n-1}A + k) \neq f(p^n A + k)$.

Следовательно, функция f удовлетворяет условиям леммы 3. Положим $B = \{p^0, p^1, \ldots, p^{n-1}\}$, тогда по лемме 3 в $M_{k,f}^B$ существуют строки каждого вида $\tilde{\alpha}^n$. Далее, так как матрица $M_{k,f}^A$ симметрична в силу коммутативности кольца A, то, следовательно, в ней имеется n строк, таких что все столбцы матрицы, образованной этими строками, различны. Значит B — диагностический тест и таблица неисправностей отделима по столбцам.

□

Стоит заметить, что теорема 6 может быть сформулирована и для более общего случая, когда в качестве кольца рассматривается такое специальное кольцо с простым идеалом p, $|A| = 2^n$, что в нём имеется цепь главных

идеалов:

$$A \supsetneq (p) \supsetneq (p)^2 \supsetneq \cdots \supsetneq (p)^{n-1} \supsetneq (p)^n = (0), a \in A.$$

В качестве примера рассмотрим источник неисправностей над кольцом $\mathbb{Z}_4[t]/(t^2+1)$. Простой идеал в этом кольце — это идеал $(t+1)$. Пусть есть какие-то булевы функции $f'(x_1, x_2, x_3, x_4)$, $f''(x_1, x_2, x_3, x_4)$ и отображения, которые переводят элементы E_2^4 в элементы кольца и, соответственно, элементы рассматриваемого кольца в E_2^4. Далее для удобства перейдём к рассмотрению функций на элементах кольца. Определим на элементах кольца функцию g, удовлетворяющую условию теоремы 6, задав её характеристическое множество $N_g = \{0, 1, 2, 3, t, t{+}1, t{+}2, t{+}3\}$. Так как $|\mathbb{Z}_4[t]/(t^2{+}1)| = 2^4$, то длина теста по теореме 6 равна четырём. Он состоит из элементов $1, 2, t, 2t$.

Также определим на элементах кольца функцию h, которая фигурирует в доказательстве леммы 2, задав её характеристическое множество $N_h = \{2t+1\}$. Так как $|\mathbb{Z}_4[t]/(t^2+1)| = 2^4$, то длина теста равна восьми. Он состоит из элементов $1, 3, t, t+2, 2t+1, 2t+3, 3t, 3t+2$.

Матрица $M^{\mathbb{Z}_4[t]/(t^2+1)}$, соответствующая таблице неисправностей, приведена в таблице 3. Строки данной матрицы, которые соответствуют тесту для функции g — в таблице 1, для h — в таблице 2. Во всех таблицах элементы кольца переобозначены латинскими буквами. Буквы, соответствующие элементам кольца, которые входят в N_f, выделены жирным шрифтом, а единственный элемент N_h обозначен символом $\mathbb{J}$.

Таблица 1

			A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	I	$\mathbb{J}$	K	L	M	N	O	P
1	=	**B**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	I	$\mathbb{J}$	K	L	M	N	O	P
2	=	**C**	**A**	**C**	**A**	**C**	I	K	I	K	**A**	**C**	**A**	**C**	I	K	I	K
t	=	**E**	**A**	**E**	I	M	**D**	**H**	L	P	**C**	**G**	K	O	**B**	**F**	$\mathbb{J}$	N
$2t$	=	I	**A**	I	**A**	I	**C**	K	**C**	K	**A**	I	**A**	I	**C**	K	**C**	K

Таблица 2

			A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	I	$\mathbb{J}$	K	L	M	N	O	P
1	=	**B**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	I	$\mathbb{J}$	K	L	M	N	O	P
3	=	**D**	**A**	**D**	**C**	**B**	M	P	O	N	I	L	K	$\mathbb{J}$	**E**	**H**	**G**	**F**
t	=	**E**	**A**	**E**	I	M	**D**	**H**	L	P	**C**	**G**	K	O	**B**	**F**	$\mathbb{J}$	N
$t+2$	=	**G**	**A**	**G**	I	O	L	N	**D**	**F**	**C**	**E**	K	M	$\mathbb{J}$	P	**B**	**H**
$2t+1$	=	$\mathbb{J}$	**A**	$\mathbb{J}$	**C**	L	**G**	P	**E**	N	I	**B**	K	**D**	O	**H**	M	**F**
$2t+3$	=	L	**A**	L	**C**	$\mathbb{J}$	O	**F**	M	**H**	I	**D**	K	**B**	**G**	N	**E**	P
$3t$	=	M	**A**	M	I	**E**	**B**	N	$\mathbb{J}$	**F**	**C**	O	K	**G**	**D**	P	L	**H**
$3t+2$	=	O	**A**	O	I	**G**	$\mathbb{J}$	**H**	**B**	P	**C**	M	K	**E**	L	**F**	**D**	N

Таблица 3

			A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	I	$\mathbb{J}$	K	L	M	N	O	P
0	=	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**
1	=	**B**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	I	$\mathbb{J}$	K	L	M	N	O	P
2	=	**C**	**A**	**C**	**A**	**C**	I	K	I	K	**A**	**C**	**A**	**C**	I	K	I	K
3	=	**D**	**A**	**D**	**C**	**B**	M	P	O	N	I	L	K	$\mathbb{J}$	**E**	**H**	**G**	**F**
t	=	**E**	**A**	**E**	I	M	**D**	**H**	L	P	**C**	**G**	K	O	**B**	**F**	$\mathbb{J}$	N
$t+1$	=	**F**	**A**	**F**	K	P	**H**	I	N	**C**	K	P	**A**	**F**	N	**C**	**H**	I
$t+2$	=	**G**	**A**	**G**	I	O	L	N	**D**	**F**	**C**	**E**	K	M	$\mathbb{J}$	P	**B**	**H**
$t+3$	=	**H**	**A**	**H**	K	N	P	**C**	**F**	I	K	N	**A**	**H**	**F**	I	P	**C**
$2t$	=	I	**A**	I	**A**	I	**C**	K	**C**	K	**A**	I	**A**	I	**C**	K	**C**	K
$2t+1$	=	$\mathbb{J}$	**A**	$\mathbb{J}$	**C**	L	**G**	P	**E**	N	I	**B**	K	**D**	O	**H**	M	**F**
$2t+2$	=	K	**A**	K	**A**	K	K	**A**	K	**A**	**A**	K	**A**	K	K	**A**	K	**A**
$2t+3$	=	L	**A**	L	**C**	$\mathbb{J}$	O	**F**	M	**H**	I	**D**	K	**B**	**G**	N	**E**	P
$3t$	=	M	**A**	M	I	**E**	**B**	N	$\mathbb{J}$	**F**	**C**	O	K	**G**	**D**	P	L	**H**
$3t+1$	=	N	**A**	N	K	**H**	**F**	**C**	P	I	K	**H**	**A**	N	P	I	**F**	**C**
$3t+2$	=	O	**A**	O	I	**G**	$\mathbb{J}$	**H**	**B**	P	**C**	M	K	**E**	L	**F**	**D**	N
$3t+3$	=	P	**A**	P	K	**F**	N	I	**H**	**C**	K	**F**	**A**	P	**H**	**C**	N	I

Глава 3

О тестах относительно сдвигов аргументов на входах схем

Текущая глава посвящена различным аспектам обнаружения и диагностики сдвигов аргументов функций.

§ 3.1. Определения и обозначения

Пусть $A = \{0,1\}$ — *алфавит*. *Слово* $\tilde{\alpha}$ — конечная последовательность символов из алфавита A, то есть $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, где $\alpha_i \in A, i = 1, \ldots, n, n \in \mathbb{N}$. *Длина слова* $\tilde{\alpha}$: $|\tilde{\alpha}| = n$. Слово длины n, которое состоит из всех нулей обозначается $\widetilde{0}^n$. Слово длины n, которое состоит из всех единиц обозначается $\widetilde{1}^n$. Пусть $\tilde{\beta} = (\beta_1, \ldots, \beta_l)$, где $\beta_j \in A, j = 1, \ldots, l, l \in \mathbb{N}$. *Конкатенация* слова $\tilde{\alpha}$ и слова $\tilde{\beta}$ — это слово $\tilde{\alpha}\tilde{\beta} = (\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_l) : |\tilde{\alpha}\tilde{\beta}| = n + l$. Слово $\tilde{\beta}$ является *подсловом* $\tilde{\alpha}$, если $\tilde{\alpha} = \tilde{\alpha}'\tilde{\beta}\tilde{\alpha}''$ для некоторых слов $\tilde{\alpha}', \tilde{\alpha}''$, быть может *пустых*, то есть не содержащих ни одного символа. Это будет обозначаться $\tilde{\beta} \sqsubset \tilde{\alpha}$. Слово $\tilde{\beta}$ является *фрагментом длины l, начинающимся с позиции* i, $1 \leqslant i \leqslant n$, $1 \leqslant l \leqslant n - i + 1$, слова $\tilde{\alpha}$, если $\beta_r = \alpha_{r'}$, где $r = 1, \ldots, l$, а $r' = i, \ldots, i + l - 1$. *Префикс* слова $\tilde{\alpha}$ — это фрагмент, начинающийся с позиции 1, *суффикс* слова $\tilde{\alpha}$ — фрагмент длины l, начинающийся с i, где $1 \leqslant i \leqslant n$, $l = n - i + 1$. *Слово $\tilde{\alpha}$ имеет период p*, $p \in \{1, \ldots, n-1\}$, тогда и только тогда, когда $(\alpha_1, \ldots, \alpha_{n-p}) = (\alpha_{p+1}, \ldots, \alpha_n)$ (см., например, [40]).

Будем считать, что слово $\tilde{\alpha}, |\tilde{\alpha}| = n$, всегда имеет *тривиальный период* n. *Слова* $\tilde{\alpha}$ *и* $\tilde{\beta}$ *равны*, если $|\tilde{\alpha}| = |\tilde{\beta}|$ и $\alpha_i = \beta_i$ для всех $i = 1, \ldots, |\tilde{\alpha}|$.

Пусть $f'(\tilde{x}^n), f''(\tilde{x}^n) \in P_2^n$. Функция $f'(\tilde{x}^n)$ *имплицирует* функцию $f''(\tilde{x}^n)$, если $N_{f'} \subset N_{f''}$.

Пусть $\tilde{\alpha} \in E_2^n$, тогда *величина* $A(\tilde{\alpha})$ — это такое максимальное число $k,\ 1 \leqslant k < n$, для которого существует число $j',\ 2 \leqslant j' \leqslant n$, такое что $(\alpha_1, \ldots, \alpha_k) = (\alpha_{j'}, \ldots, \alpha_{j'+k-1})$. Если такого k не существует, то $A(\tilde{\alpha}) = 0$.

Опишем источники неисправностей. *Источник* U^{shifts} *сдвигов переменных* действует на булеву функцию $f(x_1, \ldots, x_n)$ следующим образом. Источником выбираются число $k \in \{1, \ldots, n\}$ и набор $\widetilde{\gamma} = (\gamma_1, \ldots, \gamma_n) \in E_2^n$, и вместо вычисления $f(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ происходит вычисление $f(\alpha_{k+1}, \ldots, \alpha_n, \gamma_{n-k+1}, \ldots, \gamma_n)$. Функцию неисправности будем обозначать $f_{k,\tilde{\gamma}}(x_1, \ldots, x_n) = f(x_{k+1}, \ldots, x_n, \gamma_{n-k+1}, \ldots, \gamma_n)$.

Источник *сдвигов переменных на* k *позиций* U_k^{shifts} действует на булеву функцию $f(x_1, \ldots, x_n)$ следующим образом. Источником выбирается набор $\widetilde{\gamma} = (\gamma_1, \ldots, \gamma_k)$, и вместо вычисления $f(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ происходит вычисление $f(\alpha_{k+1}, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_k)$.

Источник *сдвигов переменных с фиксированным замещающим набором* $\tilde{\gamma}$ обозначается следующим образом: $U_{\tilde{\gamma}}^{\text{shifts}}$. Источником выбирается число $k = 1, \ldots, n$, и вместо вычисления $f(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ происходит вычисление $f(\alpha_{k+1}, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_k)$.

§ 3.2. Оценки функций Шеннона длины проверяющего и диагностического теста относительно сдвигов аргументов на входах схем

Теорема 7 (Антюфеев Г. В. [60, 63])**.** *Справедливо равенство:*

$$L^{\mathrm{detect}}(U^{\mathrm{shifts}}, n) = 2.$$

Доказательство. Рассмотрим произвольную функцию $f(\widetilde{x}^n) \in P_2^n$. Заметим, что если эта функция тождественно равна константе, то никакие сдвиги переменных $\widetilde{\gamma}$ не обнаруживаются, длина проверяющего теста в этом случае равна нулю. Будем далее считать, что у функции $f(\widetilde{x}^n)$ есть хотя бы одна существенная переменная. Пусть x_q — существенная переменная с минимальным индексом. Тогда составим множество T из произвольной пары n-разрядных двоичных наборов $\widetilde{\beta}' = (\beta_1, \ldots, \beta_{q-1}, 0, \beta_{q+1}, \ldots, \beta_n)$ и $\widetilde{\beta}'' = (\beta_1, \ldots, \beta_{q-1}, 1, \beta_{q+1}, \ldots, \beta_n)$, отличающихся лишь значениями переменной x_q и таких, что $f(\widetilde{\beta}') \neq f(\widetilde{\beta}'')$. Докажем, что T – полный проверяющий тест относительно сдвигов переменных функции $f(x_1, x_2, \ldots, x_n)$. Поскольку при любых $k = 1, \ldots, n$ и $\widetilde{\gamma} = (\gamma_1, \ldots, \gamma_n) \in E_2^n$ функция $f_{k,\widetilde{\gamma}}(x_1, \ldots, x_n) = f(x_{k+1}, \ldots, x_n, \gamma_{n-k+1}, \ldots, \gamma_n)$ существенно от переменной x_q не зависит (в силу выбора x_q), то $f_{k,\widetilde{\gamma}}(\widetilde{\beta}') = f_{k,\widetilde{\gamma}}(\widetilde{\beta}'')$, и значит, оба этих значения отличаются от одного из значений $f(\widetilde{\beta}')$ и $f(\widetilde{\beta}'')$, откуда следует верхняя оценка $L^{\mathrm{detect}}(U^{\mathrm{shift}}, n) \leqslant 2$. Нижняя оценка мгновенно получается из того, что полный проверяющий тест относительно сдвигов переменных функции $f_0(x_1, x_2, \ldots, x_n) = x_1$ не может состоять из одного набора. Теорема доказана. □

Теорема 8 (Антюфеев Г. В. [60, 63])**.** *Имеют место неравенства:*

$$c' \cdot 2^{n/2} - 1 \leqslant L^{\mathrm{diagn}}(U^{\mathrm{shifts}}, n) \leqslant c \cdot 2^{n/2},$$

где при n *нечётном* $c' = \sqrt{2}/2$ *и* $c = 2\sqrt{2}$*, а при* n *чётном* $c' = 1$ *и* $c = 3$*.*

Доказательство. Верхняя оценка. Положим $k' = \left\lfloor \frac{n}{2} \right\rfloor$. Легко видеть, что для любых $k = k', k'+1, \ldots, n$, набора $\widetilde{\gamma} = (\gamma_1, \ldots, \gamma_n) \in E_2^n$ и набора $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in E_2^n$ значение $f_{k,\widetilde{\gamma}}(\widetilde{\alpha})$ равно значению $f_{k,\widetilde{\gamma}}(\widetilde{0}^{k'}, \alpha_{k+1}, \ldots, \alpha_n)$. Поэтому все такие не равные друг другу функции неисправности $f_{k,\widetilde{\gamma}}$ заведомо попарно отличаются на наборах вида $(\widetilde{0}^{k'}, \beta_{k'+1}, \ldots, \beta_n)$ $((\beta_{k'+1}, \ldots, \beta_n) \in E_2^{n-k'})$, а число этих наборов есть $2^{n-k'} = O(\sqrt{2^n})$. Количество остальных попарно неравных функций из $F_{U^{\mathrm{shifts}}}$ не больше $2^0 + 2^1 + \ldots + 2^{k'-1} = 2^{k'} - 1$, поэтому их можно отличить друг от друга и от всех упомянутых ранее функций на не более чем $2^{k'} - 1 + \min(2^{n-k'},\ 2^{k'} - 1)$ наборах, так что всего потребуется не более $2^{n-k'} + 2^{k'} - 1 + \min(2^{n-k'},\ 2^{k'} - 1) \leqslant c \cdot 2^{n/2}$ наборов, где $c = 2\sqrt{2}$ при нечетном *n* и $c = 3$ при четном *n*. Верхняя оценка доказана.

Нижняя оценка. Рассмотрим функцию

$$h(\widetilde{x}^n) = \bigvee_{(\sigma_1,\ldots,\sigma_{k'}) \in E_2^{k'} \setminus \{\widetilde{1}^{k'}\}} x_1^{\sigma_1} x_2^{\sigma_2} \ldots x_{k'}^{\sigma_{k'}} x_{k'+1}^{\sigma_1} \ldots x_{2k'}^{\sigma_{k'}} x_{2k'+1} \ldots x_n.$$

Ясно, что $h(\widetilde{x}^n) \neq 0$ и что среди функций из $F_{U^{\mathrm{shifts}}}$ есть тождественный нуль. Замечая, что при $\widetilde{\gamma} = (\widetilde{1}^{k'}, \gamma_{k'+1}, \ldots, \gamma_{2k'}, \widetilde{1}^{n-2k'})$ и $\widetilde{\gamma} \neq \widetilde{1}^n$ функция $h_{n-k',\widetilde{\gamma}}(\widetilde{x}^n)$ отличается от тождественного нуля только на наборах вида $(\alpha_1, \ldots, \alpha_{n-k'}, \gamma_{k'+1}, \ldots, \gamma_{2k'})$, делаем вывод, что в любой диагностический тест для функции h должен войти хотя бы один набор такого вида для каждого набора $\widetilde{\gamma} = (\widetilde{1}^{k'}, \gamma_{k'+1}, \ldots, \gamma_{2k'}, \widetilde{1}^{n-2k'})$ и $\widetilde{\gamma} \neq \widetilde{1}^n$, откуда и вытекает нижняя

оценка вида $L^{\mathrm{diagn}}(U^{\mathrm{shifts}}, n) \geqslant 2^{k'} \geqslant c' \cdot 2^{n/2} - 1$, где $c' = \sqrt{2}/2$ при нечетном n и $c' = 1$ при четном n. Теорема доказана. □

Из теоремы 8 получаем следствие.

Следствие 5 (Антюфеев Г. В. [60, 63])**.** *Функция Шеннона длины диагностического теста относительно сдвигов переменных имеет следующий порядок роста:*

$$L^{\mathrm{diagn}}(U^{\mathrm{shifts}}, n) = \Theta(\sqrt{2^n}).$$

□

Теорема 9 (Антюфеев Г. В. [60])**.** *Для k, n, таких что $1 \leqslant k \leqslant n$, имеют место неравенства:*

$$\min(2^k - 1, 2^{n-k}) \leqslant L^{\mathrm{diagn}}(U_k^{\mathrm{shifts}}, n) \leqslant \min(2^k, 2^{n-k} + 1).$$

Доказательство. Верхняя оценка. Заметим, что в таблице неисправностей с учетом исходной функции имеется не более $2^k + 1$ функций, поэтому длина теста не больше, чем 2^k. С другой стороны, первые k переменных у всех функций неисправности (кроме исходной) являются фиктивными, поэтому эти функции в случае неравенства заведомо отличаются друг от друга на 2^{n-k} наборах. Еще один набор требуется, чтобы при необходимости отличить исходную функцию от единственного класса эквивалентности (по равенству) функций, не равных ей, но неотличимых от неё на выбранных 2^{n-k} наборах.

Докажем *нижнюю оценку*. Рассмотрим функцию $h(\widetilde{x}^n)$, которая равна:

$$\begin{cases} \bigvee\limits_{(\sigma_1,\ldots,\sigma_k)\in E_2^k\setminus\{(1,\ldots,1)\}} \overline{x}_1 \ldots \overline{x}_{n-2k} x_{n-2k+1}^{\sigma_1} \ldots x_{n-k}^{\sigma_k} x_{n-k+1}^{\sigma_1} \ldots x_n^{\sigma_k}, \ k \leqslant \lfloor \frac{n}{2} \rfloor, \\ \bigvee\limits_{(\sigma_1,\ldots,\sigma_{n-k})\in E_2^{n-k}} x_1^{\sigma_1} \ldots x_{n-k}^{\sigma_{n-k}} \ \overline{x}_{n-k+1} \ldots \overline{x}_k x_{k+1}^{\sigma_1} \ldots x_n^{\sigma_{n-k}}, \ k > \lfloor \frac{n}{2} \rfloor. \end{cases}$$

Рассмотрим случай $k \leqslant \left\lfloor \frac{n}{2} \right\rfloor$. Ясно, что функция $f_{k,\widetilde{1}}$ из $F_{U_k^{\text{shifts}}}$ есть тождественный нуль. Для того чтобы отличить функцию неисправности $f_{k,\widetilde{\gamma}}$ от тождественного нуля ($\widetilde{\gamma} = (\gamma_1, \ldots, \gamma_k) \neq \widetilde{1}^k$), следует включить в тест хотя бы один набор вида $(\alpha_1, \ldots, \alpha_k, \widetilde{0}^{n-2k}, \gamma_1, \ldots, \gamma_k)$, то есть в тест должно входить не менее $2^k - 1$ наборов, что меньше чем 2^{n-k}. Отсюда вытекает нижняя оценка.

Рассмотрим случай $k > \left\lfloor \frac{n}{2} \right\rfloor$. Ясно, что функция $f_{k,\widetilde{1}}$ из $F_{U_k^{\text{shifts}}}$ есть тождественный нуль. Для того чтобы отличить функцию неисправности $f_{k,\widetilde{\gamma}}$ от тождественного нуля при $\widetilde{\gamma} = \left(\widetilde{0}^{2k-n}, \gamma_{2k-n+1}, \ldots, \gamma_k\right)$ (заметим, при этом $(\widetilde{0}^{2k-n}, \gamma_{2k-n+1}, \ldots, \gamma_k) \neq \widetilde{1}^k$), следует включить в тест хотя бы один набор вида $(\alpha_1, \ldots, \alpha_{2k-n}, \gamma_{2k-n+1}, \ldots, \gamma_k)$, то есть в тест должно входить не менее 2^{n-k} наборов, что не больше чем $2^k - 1$. Отсюда вытекает *нижняя оценка*. Теорема доказана. □

Далее исследуется источник сдвигов с фиксированным замещающим набором. В качестве примера рассмотрим случай, когда $\tilde{\gamma} = (1, 1, \ldots, 1)$. В данном случае таблица неисправностей состоит из $n + 1$ столбца, то есть тривиальная верхняя оценка функции Шеннона равна n. Покажем, как построить нижнюю оценку. Рассмотрим функцию $f(\tilde{x}) = x_1 \& x_2 \& \ldots \& x_n$. Функции неисправности f^i, получающиеся из f сдвигом переменных на i, $i \in 1, 2, \ldots, n$, позиций с фиксированным замещающим набором $(1, 1, \ldots, 1)$, выглядят следующим образом: $f^i = x_{i+1} \& x_{i+2} \& \ldots \& x_n$. При $i = n$ функция f^n тождественно равна константе 1. Обозначим $f = f^0$. Функции f^i и f^j, при $i \in \{0, 1, \ldots, n-1\}$, $j \in \{1, 2, \ldots, n\}$, $i = j - 1$, отличаются только на наборах $(\underbrace{*, *, \ldots, *}_{i}, 0, 1, 1, \ldots, 1)$. Следовательно, нижняя оценка равна n. Получили точную оценку функции Шеннона длины минимального диагностического теста относительно источника сдвигов с фиксированным замещающим набором $(1, 1, \ldots, 1)$. Далее будет рассматриваться произволь-

ный замещающий набор, что существенно усложнит доказательство нижней оценки функции Шеннона.

Теорема 10 (Антюфеев Г. В. [58])**.** *Для любого $\tilde{\gamma} \in E_2^n$ справедливо неравенство:*

$$\left\lceil \frac{n}{2} \right\rceil \leqslant L^{\mathrm{diagn}}(U_{\tilde{\gamma}}^{\mathrm{shifts}}, n).$$

Доказательство. Так как на любом наборе $\tilde{\alpha} \in (\underbrace{*, \ldots, *}_{i}, \alpha_{i+1}, \alpha_{i+2}, \ldots, \alpha_n)$ значение функции $f^i(\tilde{\alpha})$, получающейся при сдвиге на i позиций, равно значению исходной функции f на наборе $(\alpha_{i+1}, \alpha_{i+2}, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_i)$, то, не ограничивая общности, будем рассматривать произвольный набор данной грани при исследовании функций $f^i(\tilde{\alpha})$.

Также, не ограничивая общности, будем рассматривать наборы $\tilde{\gamma}$, начинающиеся с единицы.

При $n = 1$ неравенство $\left\lceil \frac{n}{2} \right\rceil \leqslant L^{\mathrm{diagn}}(U_{\tilde{\gamma}}^{\mathrm{shifts}}, n)$, очевидно, выполняется. Далее считается, что $n > 1$.

Рассмотрим отдельно два случая: когда $A(\tilde{\gamma}) < \left\lfloor \frac{n}{2} \right\rfloor$, и когда $A(\tilde{\gamma}) \geqslant \left\lfloor \frac{n}{2} \right\rfloor$. Заметим, что случай $A(\tilde{\gamma}) = 0$ является частным случаем $A(\tilde{\gamma}) < \left\lfloor \frac{n}{2} \right\rfloor$.

Случай первый. Пусть $A(\tilde{\gamma}) = k < \left\lfloor \frac{n}{2} \right\rfloor$. Положим $\tilde{1} = \underbrace{(1, \ldots, 1)}_{n}$. Рассмотрим функцию $h(x_1, \ldots, x_n) \in P_2^n$:

$$h(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_n) \sqsubset \tilde{1}\tilde{\gamma}} x_1^{\sigma_1} \& \ldots \& x_n^{\sigma_n}.$$

Функцию, полученную из $h(x_1, \ldots, x_n)$ сдвигом на i, $i = 1, \ldots, n$, позиций с фиксированным замещающим набором $\tilde{\gamma}$, будем обозначать $h^i(x_1, \ldots, x_n) = h(x_{i+1}, x_{i+2}, \ldots, x_n, \gamma_1, \ldots, \gamma_i)$.

Рассмотрим множество функций h^i, где $n \geqslant i > k$. Функцию $h^i(x_1, \ldots, x_n) = h(x_{i+1}, x_{i+2}, \ldots, x_n, \gamma_1, \ldots, \gamma_i)$ можно представить следу-

ющим образом:

$$h^i(x_1,\dots,x_n) = \bigvee_{(\sigma_1,\dots,\sigma_n)\sqsubset\tilde{1}\tilde{\gamma}} x_{i+1}^{\sigma_1}\&\dots\&x_n^{\sigma_{n-i}}\&\gamma_1^{\sigma_{n-i+1}}\&\dots\&\gamma_i^{\sigma_n}$$

Исследуем характеристическое множество N_{h^i}.

Пусть есть некоторый набор $\tilde{\alpha}$, такой что $h^i(\tilde{\alpha}) = 1$. Это значит, что $h^i(\alpha_1,\dots,\alpha_n) = h(\alpha_{i+1},\alpha_{i+2},\dots,\alpha_n,\gamma_1,\dots,\gamma_i) = 1$. Введём обозначение $\tilde{\alpha}_{i,\tilde{\gamma}} = (\alpha_{i+1},\dots,\alpha_n,\gamma_1,\dots,\gamma_i)$. По определению функции h набор $\tilde{\alpha}_{i,\tilde{\gamma}} \sqsubset \tilde{1}\tilde{\gamma}$. Таким образом, для построения характеристического множества N_{h^i} требуется найти подслова длины n слова $\tilde{1}\tilde{\gamma}$, оканчивающиеся на $(\gamma_1,\dots,\gamma_i)$.

Функция h равна единице на наборе $\tilde{1}_{n-i} = (\underbrace{1,\dots,1}_{n-i},\gamma_1,\dots,\gamma_i)$. Это, очевидно, следует из самого определения функции h. Покажем, что не существует набора $\tilde{\alpha}' \in E_2^n$, удовлетворяющего одновременно следующим условиям:

- $\tilde{\alpha}' \neq \tilde{1}_{n-i}$;
- $(\alpha'_{n-i+1},\dots,\alpha'_n) = (\gamma_1,\dots,\gamma_i)$;
- $h(\tilde{\alpha}') = 1$.

Рассмотрим фрагменты длины n слова $\tilde{1}\tilde{\gamma}$, начинающиеся с позиции j такой, что $j = 1,\dots,n+1$, $j-1 \neq i$ (далее отдельно будет рассмотрено два подслучая в зависимости от ограничения на j). Предположим, что среди рассматриваемых фрагментов имеется слово $\tilde{\beta} = (\beta_1,\dots,\beta_{n-i},\gamma_1,\dots,\gamma_i) = (\beta'_1,\dots,\beta'_{n-j+1},\gamma_1,\dots,\gamma_{j-1}) \neq \tilde{1}_{n-i}$ и $h(\tilde{\beta}) = 1$.

Пусть $j > k+1$. Так как $\tilde{\beta} = (\beta_1,\dots,\beta_{n-i},\gamma_1,\dots,\gamma_i) = (\beta'_1,\dots,\beta'_{n-j+1},\gamma_1,\dots,\gamma_{j-1})$ и $i \neq j-1$, то при $i < j-1$ получается равенство $(\gamma_1,\dots,\gamma_i) = (\gamma_{j-1-i+1},\dots,\gamma_{j-1})$, а при $i > j-1$ получается равенство

$(\gamma_1, \ldots, \gamma_{j-1}) = (\gamma_{i-(j-1)+1}, \ldots, \gamma_i)$. Но тогда в обоих случаях $A(\tilde{\gamma}) > k$, что приводит к противоречию.

Фрагменты, начинающиеся с позиции j такой, что $j \leqslant k+1$, — это фрагменты вида $\tilde{\beta} = \tilde{1}_{n-j+1} = (\underbrace{1, \ldots, 1}_{n-j+1}, \gamma_1, \ldots, \gamma_{j-1})$. Предположим, что $\tilde{1}_{n-j+1}$ оканчивается на $(\gamma_1, \ldots, \gamma_i)$.

Тогда для $i-j+1 > 0$ выполняется: $(\gamma_1, \ldots, \gamma_i) = (\underbrace{1, \ldots, 1}_{i-j+1}, \gamma_1, \ldots, \gamma_{j-1})$, так как $j \leqslant k+1, n \geqslant i > k$. Следовательно, по определению $(\gamma_1, \ldots, \gamma_i)$ имеет период $i-j+1$, и $\tilde{1}_{n-j+1} = \tilde{1}$, $\tilde{1}_{n-i} = \tilde{1}$ и $\tilde{1}_{n-j+1} = \tilde{1}_{n-i}$.

Следовательно, $h^i(x_1, \ldots, x_n) = x_{i+1} \& \ldots \& x_n$ (при $i = n$ функция h^n тождественно равна единице). Так как $n \geqslant i > k$, а $k < \lfloor \frac{n}{2} \rfloor$, то количество функций неисправности такого вида не меньше, чем $\lceil \frac{n}{2} \rceil + 1$. В соответствии с определением функция $h^i(\tilde{x})$ имплицирует функцию $h^{i+1}(\tilde{x})$ при $n-1 \geqslant i > k$. Значит, для того чтобы отличить эти функции друг от друга потребуется минимум $\lceil \frac{n}{2} \rceil$ наборов.

Случай второй. $A(\tilde{\gamma}) = k \geqslant \lfloor \frac{n}{2} \rfloor$. По определению $A(\tilde{\gamma})$ существует такое j', что $(\gamma_1, \ldots, \gamma_k) = (\gamma_{j'}, \ldots, \gamma_{j'+k-1})$.

Префикс $(\gamma_1, \ldots, \gamma_{j'+k-1})$ имеет период $j'-1$. Это следует из того, что $(\gamma_1, \ldots, \gamma_{(k+j'-1)-(j'-1)}) = (\gamma_{(j'-1)+1}, \ldots, \gamma_{j'+k-1})$.

Для продолжения доказательства и удобства чтения некоторые утверждения будут оформлены в виде лемм. Некоторые из них могут выглядеть очевидными, однако, учитывая определение периода, данное выше, решено провести формальное доказательство лемм.

Лемма 4. *Пусть слово $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ имеет период p. Тогда все подслова длины, не меньшей чем p, слóва $\tilde{\alpha}$ имеют период p.*

Доказательство. По определению все подслова длины, равной p, имеют тривиальный период p. Докажем лемму для длин, бóльших p. Так как слово $\tilde{\alpha}$ имеет период p, то по определению $(\alpha_1, \ldots, \alpha_{n-p}) = (\alpha_{p+1}, \ldots, \alpha_n)$. Рас-

смотрим слово $\tilde{\beta} = (\alpha_i, \ldots, \alpha_{i+k-1}) \sqsubset \tilde{\alpha}$, где $i \in \{1, \ldots, n-k+1\}$, а $k \in \{p+1, \ldots, n\}$. Если слово $\tilde{\beta}$ имеет период p, то должно выполняться $(\alpha_i, \ldots, \alpha_{i+k-1-p}) = (\alpha_{i+p}, \ldots, \alpha_{i+k-1})$. Равенство следует из равенства $(\alpha_1, \ldots, \alpha_{n-p}) = (\alpha_{p+1}, \ldots, \alpha_n)$, так как $(\alpha_i, \ldots, \alpha_{i+k-1-p}) \sqsubset (\alpha_1, \ldots, \alpha_{n-p})$, а $(\alpha_{i+p}, \ldots, \alpha_{i+k-1}) \sqsubset (\alpha_{p+1}, \ldots, \alpha_n)$. Лемма доказана. □

Неравные подслова длины p какого-то слова, которое имеет период p, могут иметь равные суффиксы. В слове $(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$, которое имеет период, равный четырём, такими подсловами будут $(1, 0, 1, 1)$ и $(0, 1, 1, 1)$, у которых имеются равные суффиксы $(1, 1)$. Встаёт вопрос о том, при каких длинах подслов и их равных суффиксов можно утверждать о равенстве самих подслов. Следующая лемма отвечает на данный вопрос.

Лемма 5. *Пусть слово $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ имеет период p. Тогда все подслова длины l, $l \geqslant p$, сло́ва $\tilde{\alpha}$, имеющие равные суффиксы длины p, равны.*

Доказательство. Рассмотрим начинающиеся с разных позиций фрагменты $(\alpha_i, \ldots, \alpha_{i+l-1})$ и $(\alpha_j, \ldots, \alpha_{j+l-1})$, где $i = 1, \ldots, n-l+1, j = 1, \ldots, n-l+1$, $i \neq j$. Не ограничивая общности, будем полагать, что $i < j$.

Так как $l \geqslant p$, то по лемме 4 рассматриваемые подслова имеют период p. Равенство рассматриваемых подслов следует из определения периода и равенства их суффиксов длины p. Лемма доказана. □

Рассмотрим функцию $g(x_1, \ldots, x_n) \in P_2^n$:

$$g(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_n) \sqsubset \tilde{\beta}\tilde{\gamma}} x_1^{\sigma_1} \& \ldots \& x_n^{\sigma_n},$$

где $\tilde{\beta} \in E_2^n$ и имеет период $j' - 1$ и $(\beta_{n-(j'-1)+1}, \ldots, \beta_n) = (\gamma_1, \ldots, \gamma_{j'-1})$.

Рассмотрим множество функций g^i, где $n \geqslant i \geqslant \left\lfloor \frac{n}{2} \right\rfloor$. Функцию $g^i(x_1, \ldots, x_n) = g(x_{i+1}, \ldots, x_n, \gamma_1, \ldots, \gamma_i)$ можно представить следующим

образом:

$$g^i(x_1,\dots,x_n) = \bigvee_{(\sigma_1,\dots,\sigma_n)\sqsubset\tilde{\beta}\tilde{\gamma}} x_{i+1}^{\sigma_1}\&\dots\&x_n^{\sigma_{n-i}}\&\gamma_1^{\sigma_{n-i+1}}\&\dots\&\gamma_i^{\sigma_n}.$$

Исследуем характеристическое множество N_{g^i}. Предположим, что функция g^i равна единице на каком-то произвольном наборе $\tilde{\alpha}$, который при сдвиге на i с фиксированным замещающим набором $\tilde{\gamma}$ переходит в набор $\tilde{\alpha}_{i,\tilde{\gamma}} = (\alpha_{i+1},\dots,\alpha_n,\gamma_1,\dots,\gamma_i)$. По определению функции g набор $\tilde{\alpha}_{i,\tilde{\gamma}} \sqsubset \tilde{\beta}\tilde{\gamma}$. Таким образом, для построения характеристического множества N_{g^i} требуется найти подслова длины n слова $\tilde{\beta}\tilde{\gamma}$, оканчивающиеся на $(\gamma_1,\dots,\gamma_i)$.

Функция g равна единице на наборе $\tilde{\beta}_{n-i} = (\beta_{i+1},\dots,\beta_n,\gamma_1,\dots,\gamma_i)$. Покажем, что не существует набора $\tilde{\alpha}' \in E_2^n$, удовлетворяющего одновременно следующим условиям:

- $\tilde{\alpha}' \neq \tilde{\beta}_{n-i}$;
- $(\alpha'_{n-i+1},\dots,\alpha'_n) = (\gamma_1,\dots,\gamma_i)$;
- $g(\tilde{\alpha}') = 1$.

Рассмотрим в зависимости от положения фрагментов длины n сло́ва $\tilde{\beta}\tilde{\gamma}$, начинающихся с позиции $j, j \neq i+1, j = 1,\dots,n+1$, и в зависимости от диапазона i отдельно следующие подслучаи. Первый: $i, j-1 > k$; второй: $i, j-1 \leqslant k+j'-1$; третий: $i \leqslant k$ и $j-1 > k+j'-1$; четвёртый: $j-1 \leqslant k$ и $i > k+j'-1$. Третий и четвёртый подслучаи имеют место при $k+j'-1 < n$.

В первом подслучае, когда $i, j-1 > k$, если фрагмент слова $\tilde{\beta}\tilde{\gamma}$, начинающийся с j, оканчивается на $(\gamma_1,\dots,\gamma_i)$, то $(\gamma_1,\dots,\gamma_i) = (\gamma_{j-i+1},\dots,\gamma_{j-1})$ и, следовательно, $A(\tilde{\gamma}) \geqslant i$, а так как $i > k$, то возникает противоречие с $A(\tilde{\gamma}) = k$.

Во втором подслучае, когда $i, j-1 \leqslant k+j'-1$, отдельно рассмотрим ситуацию при нечётном n, $k = \left\lfloor \frac{n}{2} \right\rfloor$ и $j' = k+2$. Тогда по определению

$\tilde{\gamma}$ имеет период $k+1$. Подставляем значение периода в определение $\tilde{\beta}$ и получаем, что $(\beta_{n-(k+1)+1}, \ldots, \beta_n) = (\gamma_1, \ldots, \gamma_{k+1})$. То есть $\beta_n = \gamma_{k+1}$. Тогда $(\beta_n, \gamma_1, \gamma_2, \ldots, \gamma_k) = (\gamma_{k+1}, \gamma_{k+2}, \ldots, \gamma_n)$. И по лемме 5 получаем, что рассматриваемый фрагмент, начинающийся с j, равен $\tilde{\beta}_{n-i}$.

Теперь рассмотрим оставшиеся диапазоны. Если фрагмент, начинающийся с j, оканчивается на $(\gamma_1, \ldots, \gamma_i)$, то он равен $\tilde{\beta}_{n-i}$ по лемме 5.

При $k + j' - 1 < n$ имеет место третий подслучай, когда $i \leqslant k$, а $j - 1 > k + j' - 1$.

Рассмотрим отдельно ситуацию при нечётном n, $k = \left\lfloor \frac{n}{2} \right\rfloor$ и $j' = k + 1$. Так как $i \leqslant k$, $k = \left\lfloor \frac{n}{2} \right\rfloor$ и $i \geqslant \left\lfloor \frac{n}{2} \right\rfloor$, то $i = \left\lfloor \frac{n}{2} \right\rfloor = k$. При данных условиях $j - 1 = n$. Из того, что $j' = k + 1$, следует, что $(\gamma_1, \ldots, \gamma_k) = (\gamma_{k+1}, \ldots, \gamma_{n-1})$, то есть $(\gamma_1, \ldots, \gamma_{n-1})$ имеет период k. Так как $(\gamma_1, \ldots, \gamma_i) = (\gamma_{(j-1)-i+1}, \ldots, \gamma_{(j-1)})$, то в данной ситуации получаем, что $(\gamma_1, \ldots, \gamma_k) = (\gamma_{n-k+1}, \ldots, \gamma_n)$, и, учитывая периодичность $(\gamma_1, \ldots, \gamma_{n-1})$, получаем, что $(\gamma_{k+1}, \ldots, \gamma_{n-1}) = (\gamma_{n-k+1}, \ldots, \gamma_n)$. Тогда, так как $k = \left\lfloor \frac{n}{2} \right\rfloor$, а n нечётно, получаем, что $n - k + 1 = k + 2$, и, следовательно, по определению $(\gamma_{k+1}, \ldots, \gamma_n)$ имеет период, равный единице. Отсюда следует, что $\tilde{\gamma} = (1, 1, \ldots, 1)$. А значит, $k = n - 1$, получили противоречие.

Теперь рассмотрим оставшиеся диапазоны. Заметим, что так как $(\gamma_1, \ldots, \gamma_i) = (\gamma_{(j-1)-i+1}, \ldots, \gamma_{(j-1)})$, то $(\gamma_{(j-1)-i+1}, \ldots, \gamma_{(j-1)})$ также имеет период $j' - 1$.

Покажем, что в условиях рассматриваемого подслучая, неравенство $i \geqslant j'$ всегда справедливо в ситуациях, отличных от той, при которой были выполнимы условия: n нечётно, $k = \left\lfloor \frac{n}{2} \right\rfloor$ и $j' = k + 1$.

Напомним, что $i \geqslant \left\lfloor \frac{n}{2} \right\rfloor$. Оценим j', используя неравенство, при котором имеет смысл третий рассматриваемый подслучай: $k + j' - 1 < n$. Учитывая, что $k \geqslant \left\lfloor \frac{n}{2} \right\rfloor$, получаем, что $j' < n - \left\lfloor \frac{n}{2} \right\rfloor + 1$.

Следовательно, при чётном n получается, что $j' \leqslant \frac{n}{2}$, и $i \geqslant j'$. При нечётном n получается, что $j' \leqslant \lceil \frac{n}{2} \rceil$. Ситуация, при которой $j' = \lceil \frac{n}{2} \rceil$ была рассмотрена выше. Значит остаётся рассмотреть $j' \leqslant \lfloor \frac{n}{2} \rfloor$. В таком случае, очевидно, что неравенство $i \geqslant j'$ выполняется.

По лемме 4, так как слово $(\gamma_{k+1}, \ldots, \gamma_{k+(j'-1)+1})$ имеет длину j' и является подсловом слова $(\gamma_{(j-1)-i+1}, \ldots, \gamma_{(j-1)})$, которое имеет длину i, то слово $(\gamma_{k+1}, \ldots, \gamma_{k+(j'-1)+1})$ должно иметь период $j' - 1$. Но это не так, так как из того, что $A(\tilde{\gamma}) = k$, следует, что $\gamma_{k+(j'-1)+1} \neq \gamma_{k+1}$.

При $k + j' - 1 < n$ имеет место четвёртый подслучай, когда $j - 1 \leqslant k$, а $i > k + j' - 1$. Так как $j - 1 \leqslant k$, то по лемме 4 $(\beta_{n-i+j}, \ldots, \beta_n, \gamma_1, \ldots, \gamma_{j-1})$ имеет период $j' - 1$. Учитывая то, что $(\gamma_1, \ldots, \gamma_i) = (\beta_{n-i+j}, \ldots, \beta_n, \gamma_1, \ldots, \gamma_{j-1})$, подслово $(\gamma_1, \ldots, \gamma_i)$ также имеет период $(j' - 1)$. Отсюда получаем, что $A(\tilde{\gamma}) > k$. Снова противоречие.

Следовательно, $h^i(x_1, \ldots, x_n) = x_{i+1}^{\beta_{i+1}} \& \ldots \& x_n^{\beta_n}$ (при $i = n$ функция h^n тождественно равна единице). Так как $n \geqslant i \geqslant \lfloor \frac{n}{2} \rfloor$, то количество функций неисправности такого вида $\lceil \frac{n}{2} \rceil + 1$. Значит, для того чтобы отличить эти функции друг от друга, требуется как минимум $\lceil \frac{n}{2} \rceil$ наборов. Теорема доказана. □

Следствие 6 (Антюфеев Г. В. [58])**.** *Для любого $\tilde{\gamma} \in E_2^n$ функция Шеннона длины диагностического теста относительно сдвигов переменных с фиксированным замещающим набором имеет следующий порядок роста:*

$$L^{\mathrm{diagn}}(U_{\tilde{\gamma}}^{\mathrm{shifts}}, n) = \Theta(n).$$

Доказательство. Доказательство *верхней оценки* следует из мощностных соображений ($|F_{U_{\tilde{\gamma}}^{\mathrm{shifts}}}| \leqslant n + 1$). Доказательство *нижней оценки* следует из теоремы 10. Следствие доказано. □

§ 3.3. Легкотестируемость

Рассмотрим булеву функцию $g(\tilde{x}^n) \in P_2^n$, для которой справедливо выполнение следующих двух условий. Для любого $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \in E_2^n$ на наборах вида $(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n)$, $(0, \alpha_1, \ldots, \alpha_{n-1})$, $(1, \alpha_1, \ldots, \alpha_{n-1})$ функция $g(\tilde{x}^n) \in P_2^n$ принимает оба значения. И для любого $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \in E_2^n$ на наборах $(0, 0, \alpha_1, \ldots, \alpha_{n-2})$, $(0, 1, \alpha_1, \ldots, \alpha_{n-2})$, $(1, 0, \alpha_1, \ldots, \alpha_{n-2})$, $(1, 1, \alpha_1, \ldots, \alpha_{n-2})$ функция $g(\tilde{x}^n)$ принимает также оба значения. Оценим количество таких функций от n переменных, $n > 1$.

Под оба условия точно попадают все функции, которые линейно зависят от x_1. Таких функций $2^{2^{(n-1)}}$. Далее, учитывая второе условие, получаем, что верхняя оценка для количества таких функций равна $14^{2^{(n-2)}}$. Значит, количество таких функций заключено в интервале от $2^{2^{(n-1)}}$ до $2^{\frac{\log 14}{2} 2^{(n-1)}}$. Такие функции будут легкотестируемыми, они фигурируют в следующей теореме.

Теорема 11 (Антюфеев Г. В. [57, 61])**.** *Пусть $n > 1$ и на произвольную булеву функцию $f(\tilde{x}^n)$ действует источник неисправностей $U_{\tilde{\gamma}}^{shifts}$. Если таблица неисправностей, соответствующая $U_{\tilde{\gamma}}^{shifts}$, отделима по столбцам для любого $\tilde{\gamma}$, тогда для каждого $\tilde{\gamma}$ справедливо неравенство:*

$$L^{\mathrm{diagn}}(U_{\tilde{\gamma}}^{\mathrm{shifts}}, f(\tilde{x}^n)) \leqslant 2 \log_2 \left\lfloor \frac{n}{2} \right\rfloor + 3.$$

Перед доказательством теоремы 11 докажем следующую лемму.

Лемма 6. *Для целого n, $n > 1$, справедливо следующее неравенство:*

$$\left\lceil \log \left\lceil \frac{n+1}{2} \right\rceil \right\rceil + \left\lceil \log \left\lfloor \frac{n+1}{2} \right\rfloor \right\rceil + 1 \leqslant 2 \log \left\lfloor \frac{n}{2} \right\rfloor + 3.$$

Доказательство. Пусть $n = 2l + 1$, где l — натуральное число. Подставим n в левую часть неравенства:

$$\lceil \log(l+1) \rceil + \lceil \log(l+1) \rceil + 1 = 2 \lceil \log(l+1) \rceil + 1.$$

Подставим n в правую часть неравенства: $2 \log l + 3$. Получаем:

$$2 \lceil \log(l+1) \rceil + 1 \leqslant 2 \log l + 3,$$
$$\lceil \log(l+1) \rceil \leqslant \log l + 1.$$

Пусть m — целое неотрицательное число. Рассмотрим следующие диапазоны для l.

При $l = 2^m$ получаем неравенство $\lceil m + 1 \rceil \leqslant m + 1$, которое верно, так как m — целое число.

При $l + 1 = 2^m$ получаем верное неравенство $m \leqslant \log(2^m - 1) + 1$.

При $l \in [2^{m-1} + 1; 2^m - 2]$ получим, что $m \leqslant 1 + \log l$, то есть, что $l \geqslant 2^{m-1}$. Справедливость этого неравенства следует из выбранного диапазона.

Таким образом, лемма доказана для случая, когда n нечётно. Пусть теперь $n = 2l$, где l — натуральное число. Подставим n в левую часть неравенства:

$$\lceil \log l \rceil + \lceil \log(l+1) \rceil + 1.$$

Подставим n в правую часть неравенства: $2 \log l + 3$. Покажем, что:

$$\lceil \log l \rceil + \lceil \log(l+1) \rceil + 1 \leqslant 2 \log l + 3.$$

Пусть m — целое неотрицательное число. Рассмотрим следующие диапазоны для l.

При $l = 2^m$ получаем неравенство $m+m+1 \leqslant 2m+2$, которое, очевидно, выполняется.

При $l + 1 = 2^m$ получаем неравенство

$$\lceil \log l \rceil + \lceil \log(l+1) \rceil + 1 \leqslant m + m + 1 \leqslant 2 \log l + 3.$$

Следовательно, $m \leqslant \log l + 1$, что верно, так как $l + 1 = 2^m$.

При $l \in [2^{m-1} + 1; 2^m - 2]$ получим, что $m + m \leqslant 2 \log l + 2$, то есть, что $l \geqslant 2^{m-1}$. Справедливость этого неравенства следует из выбранного диапазона.

Таким образом, доказательство для случая, когда n чётно, завершает доказательство леммы. Лемма доказана. □

Перейдём к доказательству теоремы 11.

Доказательство. (*Теорема 11. Способ 1.)*

Таблицы неисправностей, которые соответствуют источнику неисправностей $U^{\text{shifts}}_{\tilde{\gamma}}$, действующему на функцию f, обозначим $M_{f,\tilde{\gamma}}$. Они имеют $n + 1$ столбец: n функций неисправности и исходная функция. Нумерация столбцов начинается с нуля, нулевой столбец соответствует исходной функции $f(\tilde{x}^n) \in P_2^n$, k-ый — функции $f^k_{\tilde{\gamma}}(\tilde{x}^n) \in P_2^n$, получающейся из исходной сдвигом аргументов с фиксированным замещающим набором $\tilde{\gamma}$ на k позиций, где $k \in \{1, \ldots, n\}$.

Функция $f(\tilde{x}^n) \in P_2^n$ *обладает свойством* $A1$, если для любого $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \in E_2^n$ на наборах вида $(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n)$, $(0, \alpha_1, \ldots, \alpha_{n-1})$, $(1, \alpha_1, \ldots, \alpha_{n-1})$ функция $f(\tilde{x}^n) \in P_2^n$ принимает оба значения.

Лемма 7. *Свойство* $A1$ *является необходимым для того, чтобы для любого набора* $\tilde{\gamma} = (\gamma_1, \ldots, \gamma_n) \in E_2^n$ *все столбцы таблицы неисправностей* $M_{f,\tilde{\gamma}}$ *были различны.*

Доказательство. Так как таблица неисправностей отделима по столбцам, то последние два столбца — n-ый и $(n-1)$-ый столбцы различны. Последний столбец задаётся функцией $f^n_{\tilde{\gamma}} = f(\gamma_1, \ldots, \gamma_n) \equiv \sigma_1$, $\sigma_1 \in E_2$, предпоследний — функцией $f^{n-1}_{\tilde{\gamma}} = f(x_n, \gamma_1, \ldots, \gamma_{n-1})$.

Возможны два случая.

1. $f^{n-1}_{\tilde{\gamma}} \equiv \sigma_2$, $\sigma_2 \in E_2$. Тогда, чтобы два последних столбца таблицы $M_{f,\tilde{\gamma}}$ были различны, требуется $\sigma_1 \neq \sigma_2$. Следовательно, на наборах $(\gamma_1, \ldots, \gamma_{n-1}, \gamma_n), (0, \gamma_1, \ldots, \gamma_{n-1}), (1, \gamma_1, \ldots, \gamma_{n-1})$ функция $f^n_{\tilde{\gamma}}$ должна принимать оба значения.

2. В другом случае, очевидно, выполняется свойство $A1$.

□

Функция $f(\tilde{x}^n) \in P^n_2$ обладает свойством $A2$, если для любого $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \in E^n_2$ на наборах $(0, 0, \alpha_1, \ldots, \alpha_{n-2})$, $(0, 1, \alpha_1, \ldots, \alpha_{n-2})$, $(1, 0, \alpha_1, \ldots, \alpha_{n-2})$, $(1, 1, \alpha_1, \ldots, \alpha_{n-2})$ функция $f(\tilde{x}^n)$ принимает оба значения.

Лемма 8. *Свойство $A2$ является необходимым для того, чтобы для любого набора $\tilde{\gamma} = (\gamma_1, \ldots, \gamma_n) \in E^n_2$ все столбцы таблицы неисправностей $M_{f,\tilde{\gamma}}$ были различны.*

Доказательство. Так как таблица неисправностей $M_{f,\tilde{\gamma}}$ отделима по столбцам, то последние три столбца — n-ый, $(n-1)$-ый и $(n-2)$-ый столбцы различны. Столбцы задаются следующими функциями:

- Последний: $f^n_{\tilde{\gamma}} = f(\gamma_1, \ldots, \gamma_n) \equiv \sigma_1$, $\sigma_1 \in E_2$.
- Предпоследний: $f^{n-1}_{\tilde{\gamma}} = f(x_n, \gamma_1, \ldots, \gamma_{n-1})$.
- Предпредпоследний: $f^{n-2}_{\tilde{\gamma}} = f(x_{n-1}, x_n, \gamma_1, \ldots, \gamma_{n-2})$.

Возможны два случая.

1. Пусть $f_{\tilde{\gamma}}^{n-2} \equiv \sigma_2$, $\sigma_2 \in E_2$. Отсюда следует, что $f(0,0,\gamma_1,\ldots,\gamma_{n-2}) = f(0,1,\gamma_1,\ldots,\gamma_{n-2}) = f(1,0,\gamma_1,\ldots,\gamma_{n-2}) = f(1,1,\gamma_1,\ldots,\gamma_{n-2}) = \sigma_2$. По лемме 7 из отделимости таблицы неисправностей $M_{f,\tilde{\gamma}}$ следует, что $f(0,0,\gamma_1,\ldots,\gamma_{n-2}) = f(1,0,\gamma_1,\ldots,\gamma_{n-2}) \neq f(0,\gamma_1,\ldots,\gamma_{n-1})$ и что $f(0,1,\gamma_1,\ldots,\gamma_{n-2}) = f(1,1,\gamma_1,\ldots,\gamma_{n-2}) \neq f(1,\gamma_1,\ldots,\gamma_{n-1})$. Из этого и определения функции неисправности f^{n-1} получаем, что $f_{\tilde{\gamma}}^{n-1}(x_n,\gamma_1,\ldots,\gamma_{n-1}) \equiv \sigma_3$, $\sigma_3 \in E_2$. Но тогда, так как $\sigma_1,\sigma_2,\sigma_3 \in E_2$, либо $\sigma_2 = \sigma_1$, либо $\sigma_3 = \sigma_1$, и, следовательно, в таблице будут два одинаковых столбца. Значит $f_{\tilde{\gamma}}^{n-2} \not\equiv \sigma_2$.

2. В другом случае, очевидно, выполняется свойство $A2$.

□

Лемма 9. *Функция $f(\tilde{x}^n) \in P^2(n)$ обладает одновременно свойствами $A1$ и $A2$ тогда и только тогда, когда для любого набора $\tilde{\gamma} = (\gamma_1,\ldots,\gamma_n) \in E_2^n$ все столбцы таблицы неисправностей $M_{f,\tilde{\gamma}}$ различны.*

Доказательство. Необходимость следует из леммы 7 и леммы 8. Докажем достаточность. Предположим, что $f_{\tilde{\gamma}}^i \equiv f_{\tilde{\gamma}}^j$, где $i = \{0,1,\ldots,n-1\}$, $j = i+1$. Тогда $f(x_{i+1},x_{i+2},\ldots,x_n,\gamma_1,\ldots,\gamma_i) = f(x_{i+2},\ldots,x_n,\gamma_1,\ldots,\gamma_{i+1})$ и $x_{i+1}-$ фиктивная переменная. Значит:

$$f(0,x_{i+2},\ldots,x_n,\gamma_1,\ldots,\gamma_i) = \\ = f(1,x_{i+2},\ldots,x_n,\gamma_1,\ldots,\gamma_i) = \\ = f(x_{i+2},\ldots,x_n,\gamma_1,\ldots,\gamma_{i+1}).$$

Подставив набор $\tilde{\alpha} = (0,\ldots,0) \in E_2^n$, получаем противоречие с леммой 7: $f(0,0,\ldots,0,\gamma_1,\ldots,\gamma_i) = f(1,0,\ldots,0,\gamma_1,\ldots,\gamma_i) = f(0,\ldots,0,\gamma_1,\ldots,\gamma_{i+1})$.

Предположим теперь, что $f^i_{\tilde{\gamma}} \equiv f^j_{\tilde{\gamma}}$, где $i = \{0, 1, \ldots, n-2\}$ и $j \geqslant i+2$. Тогда $f(x_{i+1}, x_{i+2}, \ldots, x_{j+1}, \ldots, x_n, \gamma_1, \ldots, \gamma_i) \equiv f(x_{j+1}, \ldots, x_n, \gamma_1, \ldots, \gamma_i, \ldots, \gamma_j)$ и x_{i+1}, x_{i+2} — фиктивные переменные. Взяв набор $\tilde{\alpha} = (0, \ldots, 0) \in E_2^n$, получаем, что $f(x_1, x_2, 0, \ldots, 0, \gamma_1, \ldots, \gamma_i) \equiv \sigma$, $\sigma \in E_2$. Следовательно, на наборах:

$$(0,0,0,\ldots,0,\gamma_1,\ldots,\gamma_i), (0,1,0,\ldots,0,\gamma_1,\ldots,\gamma_i),$$
$$(1,0,0,\ldots,0,\gamma_1,\ldots,\gamma_i), (1,1,0,\ldots,0,\gamma_1,\ldots,\gamma_i)$$

функция f принимает одно и то же значение. Получили противоречие с леммой 8. □

Лемма 10. *Если функция $f(\tilde{x}^n) \in P_2^n$ обладает свойством $A1$, то для любого $\tilde{\gamma} \in E_2^n$ в таблице $M_{f,\tilde{\gamma}}$ имеется строка:*

$$\tilde{\varepsilon} = \underbrace{(\varepsilon', \ldots, \varepsilon, \overline{\varepsilon}, \varepsilon, \overline{\varepsilon})}_{n+1}, \text{ где } \varepsilon' = \begin{cases} \varepsilon, & n+1 = 2k \\ \overline{\varepsilon}, & n+1 = 2k+1 \end{cases}, k \in \mathbb{N}.$$

Доказательство. Докажем индукцией по i, $i = n, n-1, \ldots, 0$, что в таблице неисправностей существует строка, в которой последние $n-i+1$ значений представляют собой строку из чередующихся нулей и единиц:

$$\tilde{\varepsilon}_i = (\delta_1^i, \ldots, \delta_i^i, \underbrace{\varepsilon_i, \ldots, \varepsilon, \overline{\varepsilon}, \varepsilon, \overline{\varepsilon}}_{n-i+1}),$$
$$\text{где } \varepsilon_i = \begin{cases} \varepsilon, & n-i+1 = 2l \\ \overline{\varepsilon}, & n-i+1 = 2l+1 \end{cases}, l \in \mathbb{N}_0,$$

и существуют какие-то константы $\delta_1^i, \ldots, \delta_i^i \in E_2$.

Покажем, что в $M_{f,\tilde{\gamma}}$ имеются все строки $\tilde{\varepsilon}_i$ (включая $\tilde{\varepsilon}$, что следует из определений, так как $\tilde{\varepsilon} = \tilde{\varepsilon}_0$).

База индукции. При $i = n$, очевидно, выбирается произвольная строка таблицы $M_{f,\tilde{\gamma}}$ в качестве строки $\tilde{\varepsilon}_n$.

Индуктивный переход. Пусть в $M_{f,\tilde{\gamma}}$ есть строка $\tilde{\varepsilon}_i$. Покажем, что тогда в $M_{f,\tilde{\gamma}}$ есть и строка $\tilde{\varepsilon}_{i-1}$. Пусть набор $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in E_2^n$ соответствует строке $\tilde{\varepsilon}_i$, тогда $f^i_{\tilde{\gamma}}(\alpha_1, \ldots, \alpha_n) = f(\alpha_{i+1}, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_i) = \varepsilon_i$.

Так как функция $f(\tilde{x}^n)$ обладает свойством $A1$, то по определению существует набор $\tilde{\alpha}' = (\alpha'_i, \alpha_{i+1}, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{i-1})$, $\alpha'_i \in E_2$, такой что $f(\alpha'_i, \alpha_{i+1}, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{i-1}) = \overline{\varepsilon}_i$.

Так как для каких-то произвольных $\alpha'_1, \ldots, \alpha'_{i-1} \in E_2$ верно, что $f(\alpha'_i, \alpha_{i+1}, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{i-1}) = f^{i-1}_{\tilde{\gamma}}(\alpha'_1, \ldots, \alpha'_{i-1}, \alpha'_i, \alpha_{i+1}, \ldots, \alpha_n)$, и $f^j_{\tilde{\gamma}}(\tilde{\alpha}) = f^j_{\tilde{\gamma}}(\alpha'_1, \ldots, \alpha'_i, \alpha_{i+1} \ldots, \alpha_n)$, $j = i, \ldots, n$, то набору $(\alpha'_1, \ldots, \alpha'_i, \alpha_{i+1}, \ldots, \alpha_n)$ соответствует строка:

$$(\delta_1^{i-1}, \ldots, \delta_{i-1}^{i-1}, \overline{\varepsilon}_i, \varepsilon_i, \ldots, \varepsilon, \overline{\varepsilon}, \varepsilon, \overline{\varepsilon}),$$

где $\delta_1^{i-1}, \ldots, \delta_{i-1}^{i-1} \in E_2$, которая и является искомой строкой $\tilde{\varepsilon}_{i-1}$, что выводится из определения:

$$\tilde{\varepsilon}_{i-1} = (\delta_1^{i-1}, \ldots, \delta_{i-1}^{i-1}, \underbrace{\varepsilon_{i-1}, \ldots, \varepsilon, \overline{\varepsilon}, \varepsilon, \overline{\varepsilon}}_{n-(i-1)+1}),$$

$$\varepsilon_{i-1} = \begin{cases} \varepsilon, & n-(i-1)+1 = 2l \\ \overline{\varepsilon}, & n-(i-1)+1 = 2l+1 \end{cases}, l \in \mathbb{N}_0.$$

То есть $\varepsilon_{i-1} = \overline{\varepsilon}_i$. □

Лемма 11. *Если функция $f(\tilde{x}^n) \in P_2^n$ обладает свойством $A2$, то для любого $\tilde{\gamma} \in E_2^n$ в таблице $M_{f,\tilde{\gamma}}$ имеется строка вида $\tilde{\varepsilon} = (\varepsilon_0, \ldots, \varepsilon_n)$, где значения координат с чётными индексами меньшими $n-1$ выбраны произвольно, либо с нечётными индексами меньшими $n-1$ выбраны произвольно.*

Доказательство. Не ограничивая общности, рассмотрим случай, когда n чётно, и докажем, что если функция $f(\tilde{x}^n)$ обладает свойством $A2$, то в таблице $M_{f,\tilde{\gamma}}$ имеется строка вида $\tilde{\varepsilon} = (\varepsilon_0, \ldots, \varepsilon_{n-2}, \varepsilon_{n-1}, \varepsilon_n)$, где значения координат с чётными индексами меньшими $n-1$ выбраны произвольно. Предположим, что произвольно выбраны $\zeta_0, \zeta_2, \ldots, \zeta_{n-2} \in E_2$, и $\varepsilon_0 = \zeta_0, \varepsilon_2 = \zeta_2, \ldots, \varepsilon_{n-2} = \zeta_{n-2}$. Докажем индукцией по i, $i = n-2, n-4, \ldots, 2$, что в таблице неисправностей существует строка $\tilde{\varepsilon}_i = (\delta_0^i, \ldots, \delta_{i-1}^i, \varepsilon_i, \ldots, \varepsilon_{n-2}, \varepsilon_{n-1}, \varepsilon_n)$, $\delta_0^i, \ldots, \delta_{i-1}^i \in E_2$.

База индукции. При $i = n-2$ строится строка

$$\tilde{\varepsilon}_{n-2} = (\delta_0^{n-2}, \ldots, \delta_{n-3}^{n-2}, \zeta_{n-2}, \varepsilon_{n-1}, \varepsilon_n).$$

Функция $f(\tilde{x}^n)$ обладает свойством $A2$, и, следовательно, функция $f_{\tilde{\gamma}}^{n-2}(x_1, x_2, \ldots, x_n)$ принимает оба значения, включая ζ_{n-2}, так как $f_{\tilde{\gamma}}^{n-2}(x_1, x_2, \ldots, x_n) = f(x_{n-1}, x_n, \gamma_1, \gamma_2, \ldots, \gamma_{n-2})$.

Индуктивный переход. Пусть в $M_{f,\tilde{\gamma}}$ есть строка $\tilde{\varepsilon}_i$. Покажем, что тогда в $M_{f,\tilde{\gamma}}$ есть и строка $\tilde{\varepsilon}_{i-2}$.

Пусть набор $\tilde{\eta} = (\eta_1, \ldots, \eta_n) \in E_2^n$ значений переменных $x_1, \ldots, x_n$ соответствует строке $\tilde{\varepsilon}_i$, тогда $f_{\tilde{\gamma}}^i(\eta_1, \ldots, \eta_n) = f(\eta_{i+1}, \ldots, \eta_n, \gamma_1, \ldots, \gamma_i) = \zeta_i$.

Так как функция $f(\tilde{x}^n)$ обладает свойством $A2$, то по определению существует набор $\tilde{\eta}' = (\eta'_{i-1}, \eta'_i, \eta_{i+1}, \ldots, \eta_n, \gamma_1, \ldots, \gamma_{i-2})$, $\eta'_{i-1}, \eta'_i \in E_2$, такой что $f(\tilde{\eta}') = \zeta_{i-2}$.

Далее, так как $f(\tilde{\eta}') = f_{\tilde{\gamma}}^{i-2}(\eta'_1, \eta'_2, \ldots, \eta'_{i-1}, \eta'_i, \eta_{i+1}, \ldots, \eta_n)$, где $\eta'_1, \ldots, \eta'_{i-2} \in E_2$, и $f_{\tilde{\gamma}}^j(\tilde{\eta}) = f_{\tilde{\gamma}}^j(\eta'_1, \eta'_2, \ldots, \eta'_{i-1}, \eta'_i, \eta_{i+1}, \ldots, \eta_n)$, $j = i, \ldots, n-2$, то набору $(\eta'_1, \eta'_2, \ldots, \eta'_{i-1}, \eta'_i, \eta_{i+1}, \ldots, \eta_n)$ соответствует искомая строка $\tilde{\varepsilon}_{i-2}$. □

Используя доказанные леммы, завершим доказательство теоремы. В таблице неисправностей $n+1$ столбец: $0, 1, 2, \ldots, n-2, n-1, n$. Количество

чётных столбцов ограничено сверху величиной $\left\lceil \frac{n+1}{2} \right\rceil$, а количество нечётных столбцов — величиной $\left\lfloor \frac{n+1}{2} \right\rfloor$.

Если таблица неисправностей, соответствующая $U_{\tilde{\gamma}}^{\text{shifts}}$, отделима по столбцам для любого $\tilde{\gamma}$, тогда f обладает свойствами $A1$ и $A2$.

Так как f обладает свойством $A2$, то по лемме 11 в таблице неисправностей есть все строки с любыми произвольно выбранными значениями координат с чётными индексами. Отсюда следует, что, чтобы отличить друг от друга все столбцы с чётными индексами, достаточно выбрать $\left\lceil \log_2 \left\lceil \frac{n+1}{2} \right\rceil \right\rceil$ наборов, так как это количество является достижимой тривиальной нижней оценкой для длины диагностических тестов. Аналогично выбирается $\left\lceil \log_2 \left\lfloor \frac{n+1}{2} \right\rfloor \right\rceil$ наборов для того, чтобы отличить друг от друга все столбцы с нечётными индексами.

Далее, для того чтобы отличить чётные столбцы от нечётных во всей таблице неисправности, понадобится строка из чередующихся нулей и единиц, существование которой следует из леммы 10.

Таким образом,

$$L^{diagn}(U_{\tilde{\gamma}}^{\text{shifts}}, f(\tilde{x}^n)) \leqslant \left\lceil \log \left\lceil \frac{n+1}{2} \right\rceil \right\rceil + \left\lceil \log \left\lfloor \frac{n+1}{2} \right\rfloor \right\rceil + 1,$$

что меньше либо равно, чем $2 \log \left\lfloor \frac{n}{2} \right\rfloor + 3$ по лемме 6.

Теорема доказана. □

Продемонстрируем то, как результаты предыдущей главы могут быть использованы для доказательства теоремы 11 другим способом.

Для произвольного набора $(\alpha_{i'_1}, \alpha_{i'_2}, \ldots, \alpha_{i'_n}) \in E_2^n$ определим функцию $\nu(\alpha_{i'_1}, \alpha_{i'_2}, \ldots, \alpha_{i'_n}) = \sum_{l=0}^{n-1} \alpha_{i'_{n-l}} 2^l = a'$, где $a' \in \mathbb{Z}_{2^n}$, и $i'_1, i'_2, \ldots, i'_n \in \mathbb{N}_0$. Определим также обратную к ν функцию: $\nu^{-1}(a') = (\alpha_{i'_1}, \alpha_{i'_2}, \ldots, \alpha_{i'_n})$, если $\nu(\alpha_{i'_1}, \alpha_{i'_2}, \ldots, \alpha_{i'_n}) = a'$.

Доказательство. (*Теорема 11. Способ 2.)*

Рассмотрим кольцо $Z = \mathbb{Z}_{2^n}$ вычетов по модулю 2^n.

Далее будет использоваться тот факт, что для $k \in \{0, 1, \ldots, n\}$ выполняется $|(2)^k| = 2^{n-k}$. В самом деле, $(2)^k$ делит Z на 2^k классов вычетов: $0 + 2^k Z, 1 + 2^k Z, \cdots, (2^k - 1) + 2^k Z$. Тогда по теореме Лагранжа $|(2)^k| = \frac{|Z|}{2^k} = 2^{n-k}$.

Несложно показать, что для произвольного $k' \in \mathbb{N}_0$ выполняется:

$$\nu(\alpha_{i'_1}, \alpha_{i'_2}, \ldots, \alpha_{i'_{k'}}, \alpha_{i'_{k'+1}}, \ldots, \alpha_{i'_n}) = \\ = \nu(\alpha_{i'_{k'+1}}, \ldots, \alpha_{i'_n}) + 2^{n-k'}\nu(\alpha_{i'_1}, \alpha_{i'_2}, \ldots, \alpha_{i'_{k'}}).$$

Положим $B = \{2^0, 2^1, \ldots, 2^n\}$. Далее пусть $h_{\tilde{\gamma}}(2^m) = \nu(\gamma_1, \ldots, \gamma_m)$, где $m = 1, \ldots, n$. При $m = 0$ положим $h_{\tilde{\gamma}}(2^m) = 0$ (также положим, что $h_{\tilde{\gamma}}(z), z \in Z \setminus B$). Таблица неисправностей для функции $f(\tilde{x}^n)$, соответствующая $U^{\text{shifts}}_{\tilde{\gamma}}$, — это $M^B_{h_{\tilde{\gamma}}, g^Z}$, где $g^Z(a') = 1$ тогда и только тогда, когда $f(\nu^{-1}(a')) = 1$. Для удобства чтения у функции g^Z будем опускать верхний индекс, то есть, например, вместо g^Z будем писать g, а вместо $M^B_{h_{\tilde{\gamma}}, g^Z}$ будем писать $M^B_{h_{\tilde{\gamma}}, g}$. Столбцы матрицы $M^B_{h_{\tilde{\gamma}}, g}$ индексируются элементами из Z, либо соответствующими им главными идеалами.

Для того чтобы при любом $\tilde{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_n) \in E_2^n$ матрица $M^B_{h_{\tilde{\gamma}}, g}$ была отделима по столбцам, необходимо и достаточно, чтобы для функции g выполнялись следующие два условия.

Первое — на элементах каждого класса вычетов $\mathfrak{L} \in Z/(2)^{n-1}$ функция g либо принимает различные значения, то есть $g(a) \neq g(b)$, где $a, b \in \mathfrak{L}$, либо $g(a) \neq g(2 \cdot a) = g(2 \cdot a + 1)$. **Второе** — функция g должна обладать свойством $\Psi^{(2)^{n-2}}$.

Покажем необходимость первого условия. Рассмотрим столбцы $(2)^{n-1}$ и $(2)^n$ матрицы $M^B_{h_{\tilde{\gamma}}}$. Столбец $(2)^{n-1}$ состоит из всех элементов класса вычетов

$(2)^{n-1}Z + h_{\tilde{\gamma}}(2^{n-1})$, который в свою очередь состоит из двух элементов. Обозначим эти элементы a и b. Столбец $(2)^n$ состоит из одного элемента класса вычетов $(2)^nZ+h_{\tilde{\gamma}}(2^n)$ кольца Z. Так как $(2)^n = (2)(2)^{n-1} = (2\cdot 2^{n-1})$, то $(2)^nZ+h_{\tilde{\gamma}}(2^n) = 2\cdot((2)^{n-1}Z+h_{\tilde{\gamma}}(2^n-1))+\nu(\gamma_n)$. Таким образом, столбец $(2)^n$ может состоять из элемента $2\cdot a = 2\cdot b$, либо $2\cdot a+1 = 2\cdot b+1$.

Следовательно, если $g(a) \neq g(b)$, то столбцы $(2)^{n-1}$ и $(2)^n$ матрицы $M^B_{h_{\tilde{\gamma}},g}$ различны. Если же $g(a) = g(b)$, то каждый из столбцов $(2)^{n-1}$ и $(2)^n$ матрицы $M^B_{h_{\tilde{\gamma}},g}$ будет состоять из одного элемента, следовательно, чтобы они были отличимы, должно выполняться $g(a) \neq g(2\cdot a) = g(2\cdot a+1)$.

Продолжая рассматривать ситуацию, при которой $g(a) = g(b)$, рассмотрим столбец $(2)^{n-2}$ матрицы $M^B_{h_{\tilde{\gamma}},g}$. Очевидно, что в таком случае он не может состоять из одного элемента. Следовательно, функция g должна обладать свойством $\Psi^{(2)^{n-2}}$, что показывает необходимость и второго условия. Таким образом, показано, что для функции g выполняются оба условия.

Покажем достаточность двух условий. Два любых соседних (не путать с определением соседних наборов) столбца $(2)^i$ и $(2)^j$ матрицы $M^B_{h_{\tilde{\gamma}},g}$, где $i = 0,1,\ldots,n-1, j = i+1$, различны. Это следует из вложенности идеалов, из первого условия и из того, что $(2)^j = (2)^{i+1} = (2)(2)^i = (2\cdot 2^i)$, а $(2)^jZ + h_{\tilde{\gamma}}(2^j) = 2\cdot((2)^iZ + h_{\tilde{\gamma}}(2^i)) + \nu(\gamma_j)$.

Покажем, что остальные столбцы матрицы $M^B_{h_{\tilde{\gamma}},g}$ также различны. Пусть теперь $0 \leqslant i \leqslant n-2, 2 \leqslant j \leqslant n, i < j-1$. Рассмотрим столбцы $(2)^i$ и $(2)^j$. Множество элементов столбца $(2)^j$ — это $(2)^jZ + \nu(\gamma_1,\ldots,\gamma_j) = (2)^2(2)^{j-i-2}(2)^iZ + \nu(\gamma_1,\ldots,\gamma_j) = (2)^2(2)^{j-i-2}(2)^iZ + (2)^{j-i}\nu(\gamma_1,\ldots,\gamma_i) + \nu(\gamma_{i+1},\ldots,\gamma_j)$. Далее, учитывая, что $j-i > 1$, выносим $(2)^{j-i}$ следующим образом: $(2)^2(2)^{j-i-2}((2)^iZ + \nu(\gamma_1,\ldots,\gamma_i)) + \nu(\gamma_{i+1},\ldots,\gamma_j)$. В получившемся выражении множество $(2)^iZ + \nu(\gamma_1,\ldots,\gamma_i)$ — это множество элементов столбца $(2)^i$. Далее, так как $i \leqslant n-2$, то $(2)^i \supset (2)^{n-2}$, и $(2)^iZ + \nu(\gamma_1,\ldots,\gamma_i) \supset (2)^{n-2}Z + \nu(\gamma_1,\ldots,\gamma_i)$. Так как функция g

обладает свойством $\Psi^{(2)^{n-2}}$, то в $(2)^{n-2}Z + \nu(\gamma_1, \ldots, \gamma_i)$ есть два элемента, на которых функция g принимает разные значения. И, следовательно, эти элементы присутствуют в столбце $(2)^i$. Покажем, что данные элементы отобразятся в столбце $(2)^j$ в один и тот же элемент кольца Z. Учитывая замечания, данные выше, можно подставить $(2)^{n-2}Z + \nu(\gamma_1, \ldots, \gamma_i)$ в $(2)^2(2)^{j-i-2}((2)^iZ + \nu(\gamma_1, \ldots, \gamma_i)) + \nu(\gamma_{i+1}, \ldots, \gamma_j)$. Получаем $(2)^2(2)^{j-i-2}((2)^{n-2}Z + \nu(\gamma_1, \ldots, \gamma_i)) + \nu(\gamma_{i+1}, \ldots, \gamma_j) = = (2)^{j-i-2}((2)^2(2)^{n-2}Z + (2)^2\nu(\gamma_1, \ldots, \gamma_i)) + \nu(\gamma_{i+1}, \ldots, \gamma_j) = (2)^{j-i-2}(0 + +(2)^2\nu(\gamma_1, \ldots, \gamma_i)) + \nu(\gamma_{i+1}, \ldots, \gamma_j)$. Следовательно, все остальные столбцы матрицы различны. Достаточность доказана.

Из того, что g принимает оба возможных значения на любых элементах $a, b, c \in Z$, таких что $2a = 2b = c$ и $a \neq b$, следует, что в $M^B_{h_{\tilde{\gamma}},g}$ имеется строка $\tilde{\mu} = (\mu_1, \mu_2, \ldots, \mu_n), \mu_i \neq \mu_{i+1}, i = 1, 2, \ldots, n-1$.

Положим $B^0 = \{2^0, 2^2, \ldots, 2^{2\left\lfloor \frac{n}{2} \right\rfloor - 2}\}$ и

$$B^1 = \begin{cases} \{2^1, 2^3, \ldots, 2^{2\left\lfloor \frac{n}{2} \right\rfloor - 3}\}, & \text{если } n \text{ чётно}, \\ \{2^1, 2^3, \ldots, 2^{2\left\lfloor \frac{n}{2} \right\rfloor - 1}\}, & \text{если } n \text{ нечётно}. \end{cases}$$

Мощности множеств $|B^0|$ и $|B^1|$ не более, чем $\left\lfloor \frac{n}{2} \right\rfloor$. Тогда по лемме 3 в $M^{B^0}_{h_{\tilde{\gamma}},g}$ и $M^{B^1}_{h_{\tilde{\gamma}},g}$ существуют строки каждого вида $\tilde{\alpha}^{|B_0|}$ и $\tilde{\alpha}^{|B_1|}$ соответственно. Следовательно, чтобы отличить столбцы в $M^{B^0}_{h_{\tilde{\gamma}},g}$, достаточно $\lceil \log \left\lfloor \frac{n}{2} \right\rfloor \rceil$ строк. Такое же количество строк достаточно для того, чтобы отличить столбцы матрицы $M^{B^1}_{h_{\tilde{\gamma}},g}$.

Добавим при чётном n столбцы $(2)^{n-1}$ и $(2)^n$ ко множествам B^1 и B^0 соответственно. При нечётном n — соответственно B^0 и B^1. Ввёдем обозначения для получившихся множеств. Положим $\widehat{B}^0 = \{2^0, 2^2, \ldots, 2^{2\left\lfloor \frac{n}{2} \right\rfloor}\}$ и

$$\widehat{B}^1 = \begin{cases} \{2^1, 2^3, \ldots, 2^{2\left\lfloor \frac{n}{2} \right\rfloor - 1}\}, & \text{если } n \text{ чётно}, \\ \{2^1, 2^3, \ldots, 2^{2\left\lfloor \frac{n}{2} \right\rfloor + 1}\}, & \text{если } n \text{ нечётно}. \end{cases}$$

Мощность множества $|B^0|$ не более, чем $\lceil \frac{n+1}{2} \rceil$, а множества $|B^1|$ не более, чем $\lfloor \frac{n+1}{2} \rfloor$.

Так как по лемме 3 в $M^{B^0}_{h_{\tilde{\gamma}},g}$ и $M^{B^1}_{h_{\tilde{\gamma}},g}$ существуют строки каждого вида $\tilde{\alpha}^{|B_0|}$ и $\tilde{\alpha}^{|B_1|}$ соответственно, то, учитывая, структуру столбцов $(2)^{n-1}$ и $(2)^n$ в $M^{B}_{h_{\tilde{\gamma}},g}$, можно строить тесты минимальной длины и для матриц $M^{\widehat{B}^0}_{h_{\tilde{\gamma}},g}$ и $M^{\widehat{B}^1}_{h_{\tilde{\gamma}},g}$. Следовательно, чтобы отличить столбцы в $M^{\widehat{B}^0}_{h_{\tilde{\gamma}},g}$, достаточно $\lceil \log \lceil \frac{n+1}{2} \rceil \rceil$ строк. Для $M^{\widehat{B}^1}_{h_{\tilde{\gamma}},g}$ достаточно $\lceil \log \lfloor \frac{n+1}{2} \rfloor \rceil$ строк.

Набор $\tilde{\mu}$ потребуется, чтобы отличить столбцы $M^{\widehat{B}^0}_{h_{\tilde{\gamma}},g}$ от столбцов $M^{\widehat{B}^1}_{h_{\tilde{\gamma}},g}$.

Таким образом,

$$L^{diagn}(U^{\text{shifts}}_{\tilde{\gamma}}, f(\tilde{x}^n)) \leqslant \left\lceil \log \left\lceil \frac{n+1}{2} \right\rceil \right\rceil + \left\lceil \log \left\lfloor \frac{n+1}{2} \right\rfloor \right\rceil + 1,$$

что меньше либо равно, чем $2 \log \lfloor \frac{n}{2} \rfloor + 3$ по лемме 6. Теорема доказана. □

Следствие 7 [57, 61]**.** *Пусть $n > 1$, и пусть на произвольную булеву функцию $f(\tilde{x}^n)$ действует источник неисправностей $U^{shifts}_{\tilde{\gamma}}$. Если таблица неисправностей, соответствующая $U^{shifts}_{\tilde{\gamma}}$, отделима по столбцам для любого $\tilde{\gamma}$, тогда для каждого $\tilde{\gamma}$ длина диагностического теста относительно сдвигов переменных с фиксированным замещающим набором имеет следующий порядок роста:*

$$L^{\text{diagn}}(U^{\text{shifts}}_{\tilde{\gamma}}, f(\tilde{x}^n)) = \Theta(\log n).$$

Доказательство. Нижняя оценка тривиальна. *Верхняя оценка* следует из теоремы 11. Теорема доказана. □

Заключение

В диссертации получен ряд результатов, которые относятся к теории контроля управляющих систем, являющейся частью математической теории управляющих систем.

Первая глава посвящена константным источникам неисправностей: источнику локальных константных k-кратных неисправностей и классическому источнику константных неисправностей.

Получены оценки функции Шеннона минимального диагностического теста относительно локальных константных k-кратных неисправностей. Для проверяющего теста относительно локальных константных k-кратных неисправностей получены асимптотически оптимальные оценки при некоторых ограничениях на число переменных и кратность k.

Продемонстрировано, как повысить нижнюю оценку функции Шеннона длины диагностического теста при константных не обязательно локальных неисправностях. Данный результат интересен тем, что, во-первых, он относится к исторически первой модели неисправностей. Во-вторых, данная модель не потеряла своей актуальности, несмотря на то что технологии сильно изменились. Возникнув более полувека назад, модель константных неисправностей продолжает описывать проблемы, возникающие на этапе создания уже современных микроэлектронных устройств, обладающих высокой степенью интеграции транзисторов.

Во второй и третьей главах исследуются мультипликативные источники неисправностей с аддитивным элементом и различные модификации источника сдвигов аргументов функций.

Получены оценки функции Шеннона длины тестов для мультипликативных источников неисправностей с аддитивным элементом и для сдвигов аргументов функции с фиксированным замещающим набором. Для обеих моделей неисправностей показано, что функции Шеннона длины диагностического теста имеют линейный порядок относительно количества функций неисправностей. Вместе с тем показано, как строить некоторые легкотестируемые функции.

Получены отличающиеся не более чем на единицу оценки функции Шеннона длины минимального диагностического теста относительно сдвигов на фиксированное число позиций. Для общего случая сдвигов аргументов функций (при произвольном числе позиций и при произвольном замещающем наборе) получено точное значение функции Шеннона длины проверяющего теста, и порядок функции Шеннона длины диагностического теста.

Развитие исследуемой области может идти по разным направлениям.

Первое направление — это улучшение уже существующих оценок. Например, сто́ит заметить, что вопрос асимптотики функции Шеннона длины диагностического теста при константных не обязательно локальных неисправностях остаётся открытым. Перспективным выглядит исследование оценок функции Шеннона длины минимального диагностического теста для сдвигов аргументов функций с фиксированным наползающим набором.

Второе направление — это исследование новых источников неисправностей, которые могут являться моделями неисправностей, встречающихся на практике. Малоисследованными остаются циклические сдвиги аргументов функций и сдвиги с фиксированным открывающимся набором. Для построения легкотестируемых функций относительно сдвигов с фиксированным

открывающимся набором рекомендуется посмотреть на методику, используемую в настоящей диссертации для построения легкотестируемых функций относительно сдвигов с фиксированным наползающим набором.

В диссертации улучшены оценки для классической модели теории контроля управляющих систем и вместе с тем получен ряд результатов для ранее не рассматриваемых моделей. Это продвигает теорию, в рамках которой проводились исследования.

Список литературы

1. Атья М., Макдональд И. Введение в коммутативную алгебру. — М.: Мир, 1972. — 160 с.

2. Беджанова С. Р. О минимальных тестах для схем, реализующих дизъюнкцию // Дискретн. анализ и исслед. опер. — 2008. — Т. 15, № 2. — С. 3–11.

3. Бородина Ю. В. Синтез легкотестируемых схем при константных неисправностях на выходах элементов : Дисс. ... к. ф.-м. н. : 01.01.09 / Бородина Юлия Владиславовна. — М.: МГУ, 2008. — 74 с.

4. Варден Б. Л. ван дер. Алгебра. — М.: Мир, 1975. — 649 с.

5. Верещагин Н. К., Шень А. Лекции по математической логике и теории алгоритмов. Часть 1. Начала теории множеств. — 3-е изд., стереотип. — М.: МЦНМО, 2008. — 128 с.

6. Вороненко А. А. Методы представления дискретных функций в задачах подсчёта, тестирования и распознавания свойств : Дисс. ... д. ф.-м. н. : 01.01.09 / Вороненко Андрей Анатольевич. — М.: МГУ, 2007. — 154 с.

7. Глазунов Н. И., Горяшко А. П. Об оценках длин обнаруживающих тестов для классов неконстантных неисправностей входов комбинационных схем // Изв. АН СССР. Сер. «Техническая кибернетика». — 1986. № 3. С. 197-200.

8. Дмитриев А. Н., Журавлев Ю. И., Кренделев Ф. П. О математических принципах классификации предметов и явлений // Дискрет. анализ. — Вып. 7. — Новосибирск: ИМ СО АН СССР, 1966. — С. 3–15.

9. Журавлев Ю. И. Об алгебраическом подходе к решению задач распознавания и классификации // Проблемы кибернетики. — Вып. 33. — М.: Наука, 1978. — С. 5–68.

10. Журавлев Ю. И., Флеров Ю. А., Вялый М. Н. Дискретный анализ. Основы высшей алгебры. — М.: Юрайт, 2018. — 223 с.

11. Зарисский О., Самюэль П. Коммутативная алгебра. — Т.1. — М.: ИЛ, 1963. — 373 с.

12. Зорич В. А. Математический анализ. — Часть I. — М.: Изд-во МЦНМО, 2020. — 564 с.

13. Икрамов А. А. О сложности тестирования логических устройств на некоторые типы неисправностей // Интеллектуальные системы. — 2013. — Т. 17, № 1–4. — С. 311–313.

14. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: построение и анализ. — М.: Вильямс, 2013. — 1323 с.

15. Кренделев Ф. П., Дмитриев А. Н., Журавлев Ю. И. Сравнение геологического строения зарубежных месторождений докембрийских конгломератов с помощью дискретной математики // Доклады АН СССР. — 1967. — Т. 173, № 5. — С. 1149–1152.

16. Кудрявцев В. Б., Андреев А. Е., Гасанов Э. Э. Теория тестового распознавания. — М.: ФИЗМАТЛИТ, 2007. — 320 с.

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

18. Кудрявцев В. Б., Гасанов Э. Э., Подколзин А. С. Интеллектуальные системы. — М.: Юрайт, 2019. — 219 с.

19. 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, кн. 2. — С. 90–97.

20. Курбацкая В. К. О тестах относительно некоторых типов неисправностей на входах схем // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2019. — № 3. — С. 29–35.

21. Лопунов М. А. О проверяющих тестах относительно локальных перестановок входов схем // Интеллектуальные системы. Теория и приложения — 2021. — Т. 25, Вып. 4. — С. 153–156.

22. Ложкин С. А. Лекции по основам кибернетики : Учебное пособие. — М.: Изд. отдел ф-та ВМиК МГУ, 2004. — 256 с.

23. Ляпунов А. А., Яблонский С. В. Теоретические проблемы кибернетики // Проблемы кибернетики. — Вып. 9. — М.: Наука, 1963. — С. 5–22.

24. Морозов Е. В. О единичных диагностических тестах относительно слипаний переменных в булевых функциях // Прикладная математика и информатика. — М.: МАКС Пресс, 2013. — № 44. — С. 103–113.

25. Морозов Е. В. О полных тестах относительно вытесняющих неисправностей входов схем // Вестн. Моск. ун-та. Сер. 1. Матем. Мех. — 2015. — № 1. — С. 55–59.

26. Морозов Е. В. О тестах относительно множественных линейных слипаниях переменных в булевых функциях // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2014. — № 1. — С. 22–25.

27. Морозов Е. В. О тестах относительно множественных монотонных симметрических слипаний переменных в булевых функциях // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2014. — № 4. — С. 20–27.

28. Носков В. Н. Диагностические тесты для входов логических устройств // Дискретный анализ. — Вып. 26. — Новосибирск: ИМ СО АН СССР, 1974. — С. 72–83.

29. Носков В. Н. О длинах минимальных единичных диагностических тестов, контролирующих работу входов логических схем // Методы дискретного анализа в синтезе управляющих систем. — Вып. 32. — Новосибирск: ИМ СО АН СССР, 1978. — С. 40–51.

30. Носков В. Н. О сложности тестов, контролирующих работу входов логических схем // Дискретный анализ. — Вып. 27. — Новосибирск: ИМ СО АН СССР, 1975. — С. 23–51.

31. Носков В. Н. Об универсальных тестах для диагностики одного класса неисправностей комбинационных схем // Методы дискретного анализа в решении экстремальных задач. — Вып. 33. — Новосибирск: ИМ СО АН СССР, 1979. — С. 41–52.

32. Нурмеев Н. Н. Об универсальных диагностических тестах для одного класса неисправностей комбинационных схем // Вероятностные методы и кибернетика. — Вып. 18. — Казань: Изд-во КазГУ, 1982. — С. 73–76.

33. Погосян Г. Р. О проверяющих тестах для логических схем. — М.: ВЦ АН СССР, 1982. — 57 с.

34. Погосян Г. Р. О сложности проверяющих тестов для логических устройств : Дисс. ... к. ф.-м. н. : 01.01.09 / Погосян Грант Рафикович. — М.: ВЦ РАН, 1982. — 73 с.

35. Попков К. А. Нижние оценки длин полных диагностических тестов для схем и входов схем. — Препринт № 60 ИПМ им. М. В. Келдыша РАН. — М.: ИПМ им. М. В. Келдыша РАН, 2016. — 12 с.

36. Попков К. А. Нижние оценки длин полных диагностических тестов для схем и входов схем // Прикладная дискретная математика. — 2016. — № 4(34). — С. 65–73.

37. Романов Д. С. О диагностических тестах относительно локальных слипаний переменных в булевых функциях // Прикладная математика и информатика. — Вып. 36. — М.: МАКС Пресс, 2010. — С. 91–98. (Перевод: Romanov D. S. Diagnostic tests for local coalescences of variables in Boolean functions // Computational Mathematics and Modeling. — 2012. — Vol. 23, Iss. 1. — Pp. 72–79.)

38. Романов Д. С. О тестах относительно перестановок переменных в булевых функциях // Прикладная математика и информатика. — Вып. 41. — М.: МАКС Пресс, 2012. — С. 113–121.

39. Чегис И. А., Яблонский С. В. Логические способы контроля работы электрических схем // Труды МИАН СССР. — Т. 51. — М.: МИАН СССР, 1958. — С. 270–360.

40. Шур А. М. Комбинаторика слов. — Екатеринбург: Издательство Уральского университета, 2003. — 96 с.

41. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2003. — 384 с.

42. Яблонский С. В., Чегис И. А. О тестах для электрических схем // Успехи матем. наук. — 1955. — Т. 10, вып. 4(66). — С. 182–184.

43. Яблонский С. В. Элементы математической кибернетики. — М.: Высшая школа, 2007. — 188 с.

44. Abramovici M., Breuer M. A., Friedman A. Digital Systems Testing and Testable Design. — Hoboken: John Wiley & Sons, Inc.,1990. — 652 p.

45. Boole G. An investigation of the laws of thought on which are founded the mathematical theories of logic and probabilities. — London: Macmillan, 1854. — 328 p.

46. Boole G. The mathematical analysis of logic, being an essay towards a calculus of deductive reasoning. — Cambridge: Macmillan, Barclay, & Macmillan, 1847. — 87 p.

47. Seligman E., Schubert T., Kumar M. V., A. K. Formal Verification An Essential Toolkit for Modern VLSI Design. — Second Edition. — Morgan Kaufmann, 2023. — 407 p.

48. Cadence Design Systems, Inc. (Cadence) JasperGold Coverage App User Guide. — San Jose, 2020. — 80 p.

49. Cadence Design Systems, Inc. (Cadence) JasperGold Functional Safety Verification App User Guide. — San Jose, 2020. — 87 p.

50. Karpovsky M. Universal tests for detection of input/output stuck-at and bridging faults. // IEEE Transactions on Computers. — 1983. — Vol. 32, Iss. 12. — Pp. 1194–1198.

51. Kuhl J. G., Reddy S. M. On the detection of terminal stuck-faults. // IEEE Transactions on Computers. — 1978. — Vol. C-27. — Pp. 467-469.

52. Ikram S., Barner C., Derrico J., Ellis J., Rowe M. Using Certitude Efficiently, SNUG, France, 2015.

53. Pezzè M., Young M. Software Testing and Analysis: Process, Principles, and Techniques. John Wiley & Sons, Inc –2008. — 542 p.

54. Wang L.-T., Chang Y.-W., Cheng K.-T.(T.) Electronic Design Automation: Synthesis, Verification, and Test. — Morgan Kaufmann, 2009. — 934 p.

55. Weiss C. D. Bound of the length of terminal stuck-fault tests // IEEE Transactions on Computers. — 1972. — Vol. C-21, No. 3. — Pp. 305–309.

56. Weste N., Harris D. CMOS VLSI Design: A Circuits and Systems Perspective. Fourth Edition. — Addison-Wesley, 2010. — 840 p.

Статьи в рецензируемых научных изданиях, определенных п. 2.3 Положения о присуждении ученых степеней в Московском государственном университете имени М. В. Ломоносова

57. Антюфеев Г. В. Диагностические тесты для дискретных функций, определённых на кольцах // Дискретная математика. — 2021. — Т. 33, вып. 1. — С. 3–11. (Перевод: Antyufeev G. V. Diagnostic tests for discrete functions defined on rings // Discrete Mathematics and Applications. — 2022. — Vol. 32, Iss. 3. — Pp. 147–153.)

58. Антюфеев Г. В. О диагностическом тесте при сдвигах с фиксированным замещающим набором // Дискретная математика. — 2020. — Т. 32, вып. 4. — С. 3–9. (Перевод: Antiufeev G. V. Diagnostic tests under shifts with fixed filling tuple // Discrete Mathematics and Applications. — 2021. — Vol. 31, Iss. 5. — Pp. 309–313.)

59. Антюфеев Г. В., Романов Д. С. О тестах относительно локальных константных неисправностей фиксированной кратности на входах схем //

Матем. заметки. — 2023. — Т. 114, № 3. — С. 458—463. (Перевод: Antyufeev G. V., Romanov D. S. On Test Sets Concerning Local Stuck-at Faults of Fixed Multiplicity at the Inputs of Circuits // Mathematical Notes. — 2023. — Vol. 114, Iss. 3. — Pp. 397–402.)

60. Антюфеев Г. В., Романов Д. С. О тестах при константных и сдвиговых неисправностях на входах схем // Прикладная математика и информатика. — Т. 64. — М.: МАКС Пресс, 2020. — С. 79–85. (Перевод: Antyufeev G. V., Romanov D. S. Tests with Stuck-At and Shift Faults on Circuit Inputs // Computational Mathematics and Modeling. — 2020. — Vol. 31, Iss. 4. — Pp. 494–500.)

Другие публикации автора по теме диссертации

61. Антюфеев Г. В. О свойстве булевых функций, гарантирующем существование логарифмических диагностических тестов относительно примитивных сдвигов переменных // Дискретные модели в теории управляющих систем: IX Международная конференция (Москва и Подмосковье, 20–22 мая 2015 г.) : Труды. — М.: МАКС Пресс, 2015. — С. 25–27.

62. Антюфеев Г. В. О тестах при сдвигах с фиксированным замещающим набором // Дискретные модели в теории управляющих систем: X Международная конференция, Москва и Подмосковье, 23–25 мая 2018 г. : Труды. — Москва: МАКС Пресс, 2018. — С. 37–40.

63. Антюфеев Г. В., Романов Д. С. О тестах относительно сдвигов переменных в булевых функциях // 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.: Изд-во мех.-мат. ф-та МГУ, 2012. — С. 163–165.

64. Антюфеев Г. В., Романов Д. С. Об оценках функции Шеннона длины диагностического теста при локальных константных неисправностях на входах схем // Вопросы радиоэлектроники. Серия ЭВТ. — 2016. — № 7. — С. 49–51.