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

На правах рукописи

Чистиков Дмитрий Викторович

Сложность тестирования бесповторных функций

01.01.09 — дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2011

Работа выполнена на кафедре математической кибернетики факультета вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова.

Научный руководитель:	доктор физико-математических наук, доцент Вороненко Андрей Анатольевич
Официальные оппоненты:	доктор физико-математических наук, профессор Алехина Марина Анатольевна
	доктор физико-математических наук Кочергин Вадим Васильевич
Ведущая организация:	Институт системного анализа РАН

Защита состоится 9 декабря 2011 г. в 11 часов на заседании диссертационного совета Д 501.001.44 при Московском государственном университете имени М. В. Ломоносова по адресу: 119991, Москва, ГСП-1, Ленинские горы, МГУ, 2-й учебный корпус, факультет вычислительной математики и кибернетики, ауд. 685. Желающие присутствовать на заседании диссертационного совета должны сообщить об этом за 2 дня по тел. (495) 939-30-10 (для оформления заявки на пропуск).

С диссертацией можно ознакомиться в библиотеке факультета ВМК МГУ. С текстом автореферата можно ознакомиться на официальном сайте факультета ВМК МГУ http://cs.msu.ru/ в разделе «Наука» — «Работа диссертационных советов» — «Д 501.001.44».

Автореферат разослан «__» ноября 2011 г.

Ученый секретарь
диссертационного совета Трифонов Н. П.

Общая характеристика работы

Актуальность темы. Задача тестирования управляющих систем была впервые подробно описана И. А. Чегис и С. В. Яблонским в 1950-х годах[1] и считается в настоящее время одной из основных задач математической кибернетики. Предложенная ими постановка, фактически дающая определение теста для матрицы, обобщает различные задачи логического контроля управляющих систем, в первую очередь — задачу проверки корректности функционирования и задачу диагностики неисправностей. Тестовый характер имеют многие задачи дискретной математики: в частности, широко известная задача о «расшифровке» неизвестной функции, решенная В. К. Коробковым и Ж. Анселем для класса монотонных булевых функций[2,3], является задачей условного диагностического тестирования.

В терминах тестов описываются многие из задач теории вычислительного обучения (computational learning theory) — возникшего за рубежом в 1980-х годах раздела машинного обучения (machine learning). Целью алгоритмов обучения с запросами (query learning — по сути *изучения*, или даже распознавания) является точная идентификация неизвестного объекта из известного множества[4,5] — такие постановки приводят к задаче диагностического тестирования. В качестве же меры сложности обучения как передачи знаний (teaching — *научения*) в этой теории используется функционал[6], совпадающий с функцией Шеннона длины проверяющего теста (наибольшей сложностью проверяющего теста среди объектов заданного размера).

В диссертации задачи тестирования изучаются для бесповторных булевых функций — классических объектов дискретной математики. Практическое

---

[1] Чегис И. А., Яблонский С. В. Логические способы контроля электрических схем // *Тр. МИАН СССР.* 1958. Т. 51. С. 270–360.

[2] Коробков В. К. Оценка числа монотонных булевых функций алгебры логики и сложности алгоритма отыскания разрешающего множества для произвольной монотонной функции алгебры логики // *Докл. АН СССР.* 1963. Т. 150, № 4. С. 744–747.

[3] Hansel G. Sur le nombre des fonctions booléennes monotones de n variables // *C. R. Acad. Sci. Paris.* 1966. Vol. 262. P. 1088–1090. (Ансель Ж. О числе монотонных булевых функций n переменных // *Кибернетический сборник*, изд-во Мир. Новая серия. Вып. 5. 1968. С. 53–57.)

[4] Angluin D. Queries and concept learning // *Machine Learning.* 1987. Vol. 2. P. 319–342.

[5] Angluin D. Computational learning theory: survey and selected bibliography // *Proc. of 24th Annual ACM STOC.* New York: ACM Press, 1992. P. 351–369.

[6] Goldman S. A., Kearns M. J. On the complexity of teaching // *Journal of Computer and System Sciences.* 1995. Vol. 50, № 1. P. 20–31.

значение разложимости функции в бесповторную суперпозицию (функциональной разделимости) было указано К. Шенноном в 1949 году[7]. Фундаментальная теорема о полной системе тождеств для бесповторных формул была доказана А. В. Кузнецовым[8]. Свойство бесповторности играет ключевую роль в задаче сравнения булевых базисов, которая была поставлена О. Б. Лупановым в начале 1960-х годов и впервые описана в работе Б. А. Субботовской[9]. Д. Ю. Черухин доказал[10], что сложность формульной реализации произвольных функций при переходе от одного базиса к другому увеличивается не более чем в фиксированное число раз тогда и только тогда, когда все функции первого базиса бесповторно выразимы во втором. Для классов функций, бесповторных в различных базисах, известен ряд характеризаций[11, 12, 13], алгоритмов распознавания и нахождения бесповторных представлений[14, 15].

Задачи, связанные с диагностическим тестированием бесповторных функций, изучались за рубежом с 1980-х годов, начиная с фундаментальной работы Л. Валианта[16]. Классические алгоритмы точной идентификации бесповторных функций с помощью запросов различных типов были разработаны Д. Англуин, Л. Хеллерштайн и М. Карпински[17]; обобщение на случай произвольного конечного базиса принадлежит Н. Бшаути, Т. Ханкоку и Л. Хел-

---

[7] Shannon C. The synthesis of two-terminal switching circuits // *Bell System Technical Journal.* 1949. Vol. 28, №1. P. 59–98. (Шеннон К. Синтез двухполюсных переключательных схем. В кн.: *Работы по теории информации и кибернетике.* М.: Изд-во иностранной литературы, 1963. С. 59–105.)

[8] Кузнецов А. В. О бесповторных контактных схемах и бесповторных суперпозициях функций алгебры логики // *Тр. МИАН СССР.* 1958. Т. 51. С. 186–225.

[9] Субботовская Б. А. О сравнении базисов при реализации функций алгебры логики формулами // *Докл. АН СССР.* 1963. Т. 149, №4. С. 784–787.

[10] Черухин Д. Ю. Алгоритмический критерий сравнения булевых базисов // *Математические вопросы кибернетики.* Вып. 8. М.: Физматлит, 1999. С. 77–122.

[11] Избранные вопросы теории булевых функций. Под ред. С. Ф. Винокурова и Н. А. Перязева. М.: Физматлит, 2001. 192 с.

[12] Karchmer M., Linial N., Newman I., Saks M., Widgerson A. Combinatorial characterization of read-once formulae // *Discrete Mathematics.* 1993. Vol. 114, №1–3. P. 275–282.

[13] Вороненко А. А., Федорова В. С., Чистиков Д. В. Повторность булевых функций в элементарном базисе // *Известия высших учебных заведений. Математика.* 2011. №11. С. 72–77.

[14] Golumbic M. C., Mintz A., Rotics U. Factoring and recognition of read-once functions using cographs and normality and the readability of functions associated with partial k-trees // *Discrete Applied Mathematics.* 2006. Vol. 154, №10. P. 1465–1477.

[15] Вороненко А. А. Распознавание бесповторности в произвольном базисе // *Прикладная математика и информатика.* Вып. 23. М.: МАКС Пресс, 2006. С. 67–84.

[16] Valiant L. G. A theory of the learnable // *Communications of the ACM.* 1984. Vol. 27. P. 1134–1142.

[17] Angluin D., Hellerstein L., Karpinski M. Learning read-once formulas with queries // *Journal of the ACM.* 1993. Vol. 40. P. 185–210.

лерштайн[18]. Известен и другой подход к идентификации неизвестной бесповторной функции, связанный с вероятностной постановкой задачи и использованием значений функции на случайно порождаемых последовательностях входных наборов[19].

Невырожденная задача проверяющего тестирования для бесповторных функций была поставлена А. А. Вороненко в 2002 году[20]. Для построения проверяющих тестов был предложен метод квадратов существенности, позволивший установить порядок роста соответствующей функции Шеннона. Точное значение было впоследствии установлено Л. В. Рябцом[21]. Известно обобщение метода квадратов существенности на случай бо́льших базисов — метод гиперкубов существенности[15], устанавливающий порядок функции Шеннона для базисов всех функций четырех и менее переменных, а также родственный метод, дающий линейные верхние и нижние оценки функции Шеннона для элементарного базиса из конъюнкции, дизъюнкции и отрицания[22].

Цель работы: изучение сложности задач тестирования бесповторных функций в различных базисах различными способами.

Методы исследования. В диссертации используются методы теории тестирования, теории дискретных функций и теории графов, а также методы линейной алгебры и теории вероятностей. Часть результатов работы непосредственно связана с использованием и развитием методов квадратов существенности и гиперкубов существенности для проверяющего тестирования бесповторных функций.

Научная новизна. Результаты диссертации являются новыми.

[18] Bshouty N. H., Hancock T. R., Hellerstein L. Learning Boolean read-once formulas over generalized bases // *Journal of Computer and System Sciences.* 1995. Vol. 50, № 3. P. 521–542.

[19] Goldman S. A., Kearns M. J., Schapire R. E. Exact identification of read-once formulas using fixed points of amplification functions // *SIAM Journal on Computing.* 1993. Vol. 22, № 4. P. 705–735.

[20] Вороненко А. А. О проверяющих тестах для бесповторных функций // *Математические вопросы кибернетики.* Вып. 11. М.: Физматлит, 2002. С. 163–176.

[21] Рябец Л. В. Сложность проверяющих тестов для бесповторных булевых функций. Серия: Дискретная математика и информатика. Вып. 18. Иркутск: Изд-во Ирк. гос. пед. ун-та, 2007. 30 с.

[22] Вороненко А. А. О длине проверяющего теста для бесповторных функций в базисе $\{0, 1, \&, \vee, \neg\}$ // *Дискретная математика.* 2005. Т. 17, № 2. С. 139–143.

Основные результаты:

1. Получены оценки, а в ряде случаев и точные значения длин проверяющих тестов для индивидуальных функций, бесповторных в базисе всех функций двух переменных и в базисе из конъюнкции и дизъюнкции.

2. Корректность метода гиперкубов существенности для проверяющего тестирования бесповторных функций доказана для базиса всех функций пяти переменных.

3. Доказано, что полиномиальная разрешимость задачи проверяющего тестирования бесповторных функций в произвольном конечном базисе является достаточным условием полиномиальной разрешимости соответствующей задачи условного диагностического тестирования с запросами тождественности.

4. Получена экспоненциальная нижняя оценка сложности условных диагностических тестов с запросами числа единиц по модулю два для функций, бесповторных в сложных неэлементарных базисах.

Практическая значимость. Диссертация носит теоретический характер. Полученные результаты могут найти применение при проектировании, прежде всего оценке априорных возможностей, управляющих систем, а также в задачах, связанных с восстановлением дискретных функций и машинным обучением.

Публикации. По теме диссертации опубликовано 13 работ, в том числе 6 работ [2; 4; 6; 7; 9; 12] в рецензируемых изданиях, включенных в перечень ВАК. Пять работ [1; 2; 4; 6; 11] опубликовано в соавторстве. В работах [1; 11] решение задачи принадлежит автору диссертации, а постановка задачи — научному руководителю. В работе [2] автору диссертации принадлежат результаты по проверяющим тестам для бесповторных функций в базисе всех функций двух переменных, в работе [4] — нижние оценки для индивидуальных функций и универсальная нижняя оценка для функций, представимых бесповторными КНФ и ДНФ. В работе [6] автору диссертации принадлежит экспоненциальная нижняя оценка сложности диагностических тестов для функций, бесповторных в неэлементарных базисах.

Апробация результатов. Результаты диссертации докладывались на следующих конференциях и семинарах:

— XVII Международная школа-семинар «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (г. Новосибирск, 27 октября — 1 ноября 2008 г.);

— XVIII Международная школа-семинар «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (г. Пенза, 28 сентября — 3 октября 2009 г.);

— 3-я Российская школа-семинар «Синтаксис и семантика логических систем» (г. Иркутск, 10–14 августа 2010 г.);

— 22-й Международный семинар по комбинаторным алгоритмам IWOCA 2011 (22nd International Workshop on Combinatorial Algorithms, г. Виктория, Британская Колумбия, Канада, 20–22 июня 2011 г.);

— 1-й Российско-финский симпозиум по дискретной математике RuFiDiM (г. Санкт-Петербург, 21–24 сентября 2011 г.);

— 13-й Международный симпозиум по символьным и численным алгоритмам для научных расчетов SYNASC 2011 (13th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, г. Тимишоара, Румыния, 26–29 сентября 2011 г.).

Кроме того, результаты обсуждались на научных семинарах кафедры математической кибернетики факультета ВМК МГУ.

Структура и объем диссертации. Работа состоит из введения, трех глав, заключения и списка литературы, содержащего 71 наименование. Диссертация содержит 5 таблиц, общий объем текста составляет 135 страниц.

Краткое содержание работы

Во введении приводится обзор исследований и известных результатов, связанных с темой диссертации, и кратко излагается содержание работы.

В главе 1 изучается задача проверяющего тестирования для функций, бесповторных в классических базисах: в базисе всех функций двух переменных, в базисе из конъюнкции, дизъюнкции и отрицания, в базисе из конъюнкции и дизъюнкции.

Параграф 1.1 посвящен основным определениям и обозначениям, связанным с задачей проверяющего тестирования бесповторных функций.

Формула $\mathcal{F}$ над базисом $\mathfrak{B}$ называется *бесповторной*, если каждая переменная встречается в $\mathcal{F}$ не более одного раза. Булева функция f называется *бесповторной* в базисе $\mathfrak{B}$, если она выразима хотя бы одной бесповторной формулой над $\mathfrak{B}$.

Пусть базис $\mathfrak{B}$ фиксирован, функция $f(x_1, \ldots, x_n)$ бесповторна в $\mathfrak{B}$ и существенно зависит от всех своих переменных. Множество входных наборов $M \subseteq \{0,1\}^n$ называется *проверяющим тестом* для функции f, если значения f на наборах из M отличают f от всех остальных бесповторных в $\mathfrak{B}$ функций, зависящих от переменных $x_1, \ldots, x_n$. Число наборов в проверяющем тесте называют его *длиной*. Минимальная длина проверяющего теста для бесповторной функции f в $\mathfrak{B}$ обозначается символом $T_{\mathfrak{B}}(f)$. Определение $T_{\mathfrak{B}}(f)$ задает функционал сложности для бесповторных функций.

Неориентированный граф $G = (X, E)$ без петель и кратных ребер называется *кографом*, если его можно преобразовать в пустой граф операциями взятия дополнения связной компоненты. Корневое дерево называется *кодеревом*, если каждая его нелистовая (*внутренняя*) вершина имеет не менее чем двух сыновей и множество всех таких вершин правильно раскрашено в два цвета $0, 1$ (соседние вершины красятся в разные цвета). Множество кографов на вершинах X и множество кодеревьев с листьями X связаны взаимно однозначным соответствием.

В §1.2 задача проверяющего тестирования бесповторных функций изучается для базиса B_2 всех функций двух переменных. Основным результатом является теорема 1.1; в ее формулировке символом $\ddot{D}_f$ обозначено кодерево, связанное с *каноническим* представлением функции f, а символом $\nu(\cdot)$ — целочисленная *характеристика* кодерева, равная минимальной длине «графового» теста для соответствующего кографа (явная формула для вычисления этой характеристики была найдена А. А. Вороненко [2]).

Теорема 1.1. [2] *Для любой бесповторной в базисе B_2 функции f справедливо неравенство*

$$T_{B_2}(f) \leqslant 4\,\nu(\ddot{D}_f).$$

Теорема 1.1 уточняет метод квадратов существенности для получения индивидуальных верхних оценок минимальной длины проверяющего теста. Немодифицированный метод[20] дает универсальную оценку $4\binom{n}{2}$; известно другое уточнение[21], приводящее к неулучшаемой в общем случае оценке $\binom{n}{2} + n + 1$.

Дерево с единственной внутренней вершиной и n листьями будем называть *n-листовой звездой.*

Теорема 1.3. [3] *Характеристика произвольного кодерева D с $n \geqslant 2$ листьями удовлетворяет двойному неравенству $2n-3 \leqslant \nu(D) \leqslant \binom{n}{2}$, нижняя граница в котором достигается на двоичных деревьях и, в случае $n = 3$, трехлистовой звезде (и только на них), а верхняя — на деревьях с одной и двумя внутренними вершинами (и только на них), причем значения $\nu(D)$ для всевозможных D с n листьями заполняют весь указанный отрезок.*

Функция Шеннона длины проверяющего теста для бесповторных функций в базисе $\mathfrak{B}$ определяется по стандартному правилу

$$T_{\mathfrak{B}}(n) \;=\; \max_{f(x_1,\ldots,x_n)} T_{\mathfrak{B}}(f),$$

где максимум берется по всем бесповторным в $\mathfrak{B}$ функциям переменных $x_1, \ldots, x_n$.

В § 1.3 задача проверяющего тестирования изучается для *элементарного базиса* $B_0 = \{\&, \vee, \neg\}$. Ранее было известно[22], что значение функции Шеннона длины проверяющего теста для функций, бесповторных в этом базисе, заключено между $n+1$ и $7/2 \cdot n$ (то же верно и для базиса $\{\&, \vee\}$). Существует не доказанная и не опровергнутая гипотеза о том, что $T_{B_0}(f) = n + 1$ для всех бесповторных в B_0 функций f, имеющих в точности n существенных переменных.

Теорема 1.4. [12] *Справедливо равенство*

$$T_{\{\&,\vee\}}(n) = n + 1.$$

Теорема 1.5. [12] *Справедливо неравенство*

$$T_{B_0}(n) \leqslant 2n+1.$$

Параграф 1.4 посвящен изучению задачи проверяющего тестирования для базиса $\{\&, \vee\}$. Везде в данном параграфе для удобства записи используется обозначение $T(f)$ вместо $T_{\{\&,\vee\}}(f)$. Символами $T_0(f)$ и $T_1(f)$ обозначается минимальное количество нулевых и соответственно единичных наборов в проверяющем тесте для f. Основная теорема 1.6 сводит задачу определения точного значения $T(f)$ минимальной длины теста к нескольким экземплярам специальной задачи комбинаторной оптимизации. Входом этой задачи является произвольное мультимножество F разбиений натуральных чисел, а оптимальное решение обозначается символом $Z(F)$.

Теорема 1.6. [13] *Пусть функция f задана соотношением*

$$f = (f_{1,1} \vee \ldots \vee f_{1,r_1}) \,\&\, (f_{2,1} \vee \ldots \vee f_{2,r_2}) \,\&\, \ldots \,\&\, (f_{l,1} \vee \ldots \vee f_{l,r_l}),$$

где $l \geqslant 2$, все $r_i \geqslant 1$, функции $f_{i,j}$ бесповторны в $\{\&, \vee\}$, не выражаются бесповторными дизъюнкциями и не имеют общих существенных переменных, причем если $r_i = 1$, то $f_{i,1}$ — переменная. Тогда

$$T(f) = T_0(f) + T_1(f),$$

$$T_0(f) = \sum_{i=1}^{l} T_0(f_i) \quad \text{и} \quad T_1(f) = Z(F),$$

где F — мультимножество разбиений $T_1(f_{i,1})+\cdots+T_1(f_{i,r_i})$ для $i = 1, \ldots, l$, а $f_i = f_{i,1} \vee \ldots \vee f_{i,r_i}$.

Отметим, что результат теоремы 1.6 непосредственно переносится на двойственный случай (меняются местами символы & и $\vee$, а также булевы константы 0 и 1).

Теорема 1.6 дает индуктивный способ получения оценок и точных значений величины $T(f)$ из оценок и соответственно точных значений величины $Z(F)$. Кроме того, показывается, что значение $Z(F)$ можно, в свою очередь, определять по значению $T(f)$ для специально подобранной f, так что задачи вычисления этих двух величин оказываются в данном смысле эквивалентны.

Следствие 1.6.1. [13] *Для всех неконстантных функций f, бесповторных в базисе $\{\&, \vee\}$, справедливо равенство*

$$T(f) = T_0(f) + T_1(f).$$

Если все компоненты каждого разбиения из F равны 1, то значение $Z(F)$ обозначается также символом $Z(r_1, \ldots, r_l)$, где $r_1, \ldots, r_l$ — соответствующие количества компонент в этих разбиениях (с учетом кратности).

Следствие 1.6.2. [13] *Для функции f, выразимой бесповторной КНФ*

$$(x_{1,1} \vee \ldots \vee x_{1,r_1}) \,\&\, (x_{2,1} \vee \ldots \vee x_{2,r_2}) \,\&\, \ldots \,\&\, (x_{l,1} \vee \ldots \vee x_{l,r_l})$$

с $l \geqslant 2$ и $r_i \geqslant 1$ для $i = 1, \ldots, l$, минимальная длина проверяющего теста определяется равенством

$$T(f) = l + Z(r_1, \ldots, r_l).$$

Теорема 1.7. [13] *Если F состоит из разбиений $m_i = t_{i,1} + \cdots + t_{i,r_i}$, где $i = 1, \ldots, l$, то*

$$Z(F) \geqslant \max\left\{ \max_i m_i,\ \max_{i \neq k}(r_i + r_k - 1),\ \log_2\left(\sum_{i=1}^{l} 2^{r_i - 1} - l + 1\right) + 1 \right\}.$$

С. Е. Бубнов доказал неравенство $T(f) \geqslant 2\sqrt{n}$, справедливое для всех бесповторных в $\{\&, \vee\}$ функций, существенно зависящих от n переменных [4]. Оценки теоремы 1.7 позволяют улучшить этот результат для функций, выразимых бесповторными монотонными КНФ и ДНФ.

Теорема 1.8. [4] *Для всех функций f, выразимых бесповторными монотонными КНФ и ДНФ и зависящих существенно от n переменных, справедливо неравенство*

$$T(f) \geqslant 2\sqrt{2}\sqrt{n} - 1.$$

Отметим, что для специальной подпоследовательности КНФ n переменных А. А. Вороненко доказал [4] верхнюю оценку $T(f) \leqslant 3\sqrt{n} - 1$, близкую к нижней границе теоремы 1.8 (теорема 1.7 обращает эту верхнюю оценку в точное равенство).

Теорема 1.9. [13] *Если* $r_1 \geqslant r_2 \geqslant \ldots \geqslant r_l$, *то*

$$Z(r_1, \ldots, r_l) \leqslant \min\left\{ \sum_{i \neq 3k} (r_i - 1),\ 4\,(\max\{r_1, l\} - 1),\ \sum_{i=1}^{\lceil \log_2(l+1) \rceil} (r_i - 1) \right\} + 1.$$

Используя следствие 1.6.2, теорему 1.9, а также известные свойства *почти всех* разбиений n-элементного множества, удается определить асимптотику величины $T(f)$ для *почти всех* функций, выразимых бесповторными монотонными КНФ (результат для ДНФ формулируется двойственным образом).

Теорема 1.10. [13] *Для почти всех функций f, выразимых бесповторными монотонными КНФ и зависящих существенно от n переменных, справедливо соотношение*

$$T(f) \sim T_0(f) \sim \frac{n}{\ln n}.$$

В главе 2 задача проверяющего тестирования изучается для случая произвольного базиса. В § 2.1 формулируются необходимые для дальнейшего изложения определения и факты. Базис всех функций l переменных при $l \geqslant 2$ обозначается символом B_l.

Множество из 2^l входных наборов, отличающихся только в компонентах с номерами $i_1, \ldots, i_l$, называется *l-мерным гиперкубом существенности* переменных $x_{i_1}, \ldots, x_{i_l}$ функции f, если остаточная подфункция f на этом множестве существенно зависит от всех своих l переменных[15].

Произвольное множество входных наборов, содержащее для каждой l-ки переменных функции f, для которой это возможно, некоторый l-мерный гиперкуб их существенности, называется *множеством l-мерных гиперкубов существенности* функции f. Предположение о том, что множества l-мерных гиперкубов существенности являются проверяющими тестами для любых бесповторных функций в базисах B_l при произвольном l, было названо *гипотезой гиперкубов существенности.* Справедливость гипотезы гиперкубов существенности означает, в частности, полиномиальность относительно n функции Шеннона длины проверяющего теста для бесповторных функций в произвольном конечном базисе. Для $l \leqslant 4$ справедливость этой гипотезы была ранее доказана А. А. Вороненко[15].

Параграф 2.2 посвящен доказательству гипотезы гиперкубов существенности для базиса B_5.

Теорема 2.1. [1] *Любое множество пятимерных гиперкубов существенности произвольной бесповторной в B_5 функции f, существенно зависящей от всех своих переменных, образует проверяющий тест:*

$$T_{B_5}(n) \leqslant 32 \binom{n}{5}.$$

Следствие 2.1.1. $T_{B_5}(n) = \Theta(n^5)$.

Базис $\mathfrak{B}$ называется *наследственным*, если с каждой функцией h он содержит все ее остаточные подфункции, получаемые подстановками констант на места переменных.

В § 2.3 устанавливается, что в широком классе базисов, вообще говоря, неверно *правило подфункции* — импликация «если f' — подфункция f, то $T_{\mathfrak{B}}(f') \leqslant T_{\mathfrak{B}}(f)$».

Теорема 2.2. [7] *Если конечный наследственный базис $\mathfrak{B}$ содержит двухместную дизъюнкцию и последовательность $T_{\mathfrak{B}}(x_1 \vee \ldots \vee x_n)/n$ не является ограниченной, то в $\mathfrak{B}$ не выполняется правило подфункции.*

Входной набор α функции f называется *изолированным*[23], если для всех соседних с ним наборов β справедливо неравенство $f(\alpha) \neq f(\beta)$.

Следствие 2.2.1. [7] *Правило подфункции не выполняется в любом конечном наследственном базисе, содержащем дизъюнкцию и какую-либо не бесповторную в $\{\&, \vee, \neg\}$ функцию, имеющую изолированный набор.*

Условия следствия 2.2.1 справедливы, в частности, для базисов B_l всех функций l переменных при любом фиксированном $l \geqslant 2$. Для базиса из конъюнкции и дизъюнкции, напротив, не выполнены даже условия теоремы 2.2, однако в нем правило подфункции удается опровергнуть с помощью результатов § 1.4.

В § 2.4 предлагается специальная постановка задачи проверяющего тестирования, в которой базис бесповторных функций выбирается с учетом тестируемой функции f. Вводится функционал $T_*(f)$, равный минимуму длины проверяющего теста f по всем наследственным базисам, содержащим f. Это

[23] Вороненко А. А. Тестирование дизъюнкции как бесповторной функции в произвольном бесповторном базисе // *Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика.* 2008. №4. С. 51–52.

равносильно выбору множества всех подфункций функции f, включая f, в качестве базиса.

Утверждение 2.4. *Справедливо соотношение*

$$\max_{f(x_1,\dots,x_n)} T_*(f) = \Omega(2^{2n/3}/\sqrt{n}),$$

где максимум берется по множеству всех булевых функций переменных $x_1, \dots, x_n$.

Теорема 2.4. [10] *При любом $n \geqslant 3$ для функции*

$$\mathrm{XOR}_n(x_1, \dots, x_n) = (x_1 \vee \dots \vee x_n) \,\&\, (\overline{x}_1 \vee \dots \overline{x}_n).$$

справедливо равенство

$$T_*(\mathrm{XOR}_n) = 5.$$

Теорема 2.5. [10] *Если $n \geqslant 5$ и функция f существенно зависит от n переменных, то*

$$T_*(f) \geqslant 5.$$

Теорема 2.6. [10] *Если $n \geqslant 5$ и для функции f, существенно зависящей от n переменных, справедливо равенство*

$$T_*(f) = 5,$$

то f либо совпадает с XOR_n, либо получается из нее переименованием переменных и навешиванием отрицаний на некоторые переменные и, возможно, на саму функцию.

Глава 3 посвящена задаче диагностического тестирования для бесповторных функций. В § 3.1 формулируется определение условного диагностического теста и описывается общая постановка задачи.

В качестве множества возможных состояний управляющей системы (допустимых объектов) рассматривается множество R_n (соответственно R'_n) всех функций, бесповторных в фиксированном базисе $\mathfrak{B}$ и зависящих произвольным (соответственно существенным) образом от переменных $x_1, \dots, x_n$. В качестве элементарных вопросов, используемых для диагностики (точной идентификации неизвестной функции из рассматриваемого множества), рассматриваются стандартные запросы значения функции в точке, а также обобщающие их запросы к подкубам булева куба $\{0,1\}^n$ — области определения неизвестной функции. Запрос, связанный с подкубом $\Gamma \in \{0, 1, -\}^n$, возвращает значение некоторого функционала от значений неизвестной функции на наборах подкуба Γ. В случае нулевой размерности подкуба возвращается значение функции в запрошенной точке.

Рассмотрим ориентированное (от корня) корневое дерево, каждой внутренней (нелистовой) вершине которого приписаны допустимый запрос, выходящим из нее дугам — все возможные ответы на этот запрос, а листьям — функции из R_n (R'_n) и символы $*$. Назовем такое дерево *условным диагностическим тестом*, если для каждого листа этого дерева ориентированный маршрут из корня в этот лист несет последовательность пометок (запрос — ответ), согласованную с пометкой этого листа f и только с ней (соответственно не согласованную ни с одной функцией f в случае пометки $*$). *Сложность* условного диагностического теста определяется как максимальное число дуг на пути от корня к листу (число вопросов, которые задает изображаемый деревом алгоритм в худшем случае). Минимальная сложность условного диагностического теста для множества R_n (R'_n) при условии, что доступны запросы типа F, обозначается символом $L^F_{\mathfrak{B}}(n)$ ($L'^F_{\mathfrak{B}}(n)$).

В § 3.2 изучаются *запросы тождественности*, возвращающие 1 для тех подкубов, на которых неизвестная функция постоянна, и 0 для всех остальных подкубов (обозначение: $\equiv$).

Теорема 3.1. [9] *Если $l < \infty$ — максимальная арность функций базиса $\mathfrak{B}$, то*

$$L^{\equiv}_{\mathfrak{B}}(n) \leqslant 2n\, T_{\mathfrak{B}}(n) + O(n^{l+2}).$$

Следствие 3.1.1. [9] *Если для конечного базиса $\mathfrak{B}$ функция Шеннона $T_{\mathfrak{B}}(n)$ длины проверяющего теста растет не быстрее некоторого полинома от n, то задача условного диагностического тестирования на множестве всех бесповторных функций в базисе $\mathfrak{B}$ с запросами тождественности решается алгоритмом полиномиальной сложности (величина $L^{\equiv}_{\mathfrak{B}}(n)$ также ограничена некоторым полиномом от n).*

Параграф 3.3 посвящен *запросам числа единиц по модулю* 2: такой запрос возвращает 1, если число единиц неизвестной функции на запрошенном подкубе нечетно, и 0 иначе (обозначение: $\oplus$). Для элементарного базиса $B_0 = \{\&, \vee, \neg\}$ А. А. Вороненко доказал [6] неравенство $L'^{\oplus}_{B_0}(n) \leqslant n^2 - n + 1$.

Теорема 3.3. [6] *Если базис* $\mathfrak{B}$ *является наследственным, допускает бесповторное выражение всех функций базиса* B_0 *и содержит хотя бы одну функцию, не являющуюся бесповторной в* B_0, *то*

$$L'^{\oplus}_{\mathfrak{B}}(n) = 2^{\Omega(n)}.$$

Следствие 3.3.1. [6] *Пусть* $\mathfrak{B}$ *— наследственный базис, допускающий бесповторное выражение всех функций базиса* B_0. *Тогда задача условного диагностического тестирования на множестве всех бесповторных функций в базисе* $\mathfrak{B}$, *существенно зависящих от переменных* $x_1, \ldots, x_n$, *с запросами числа единиц по модулю 2 решается алгоритмом полиномиальной сложности в том и только том случае, когда все функции* $\mathfrak{B}$ *бесповторны в* B_0.

В § 3.4 рассматриваются *запросы двух младших бит числа единиц*. Обращенные к подкубу $\Gamma \in \{0, 1, -\}^n$ запросы этих двух типов возвращают два младших бита s_1 и s_0 числа единиц $\overline{s_l \ldots s_1 s_0}$ неизвестной функции на запрошенном подкубе (общее обозначение для совокупности запросов k младших бит: (2^k)). Каждому биту соответствует отдельный тип запроса; запросы младшего бита s_0 — это запросы суммы по модулю 2.

Теорема 3.4. [8] *Справедливо неравенство*

$$L'^{(4)}_{B_0}(n) \leqslant \frac{3}{4} \cdot n^2 - \frac{1}{2} \cdot n + 1.$$

Теорема 3.4 показывает, что в случае элементарного базиса возможность запрашивать значения s_1 (в дополнение к s_0) позволяет сократить сложность условного диагностического теста примерно на четверть.

В заключении приводится краткое обсуждение основных результатов диссертации и даются рекомендации по использованию научных выводов.

Публикации по теме диссертации

1. Вороненко А. А., Чистиков Д. В. О тестировании бесповторных булевых функций в базисе B_5 // *Материалы XVII Международной школы-семинара «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (Новосибирск, 27 октября – 1 ноября 2008 г.).* Новосибирск: Изд-во ИМ СО РАН, 2008. С. 24–30.

2. Вороненко А. А., Чистиков Д. В. Индивидуальное тестирование бесповторных функций // *Ученые записки Казанского государственного университета. Сер. Физико-математические науки.* 2009. Т. 151, кн. 2. С. 36–44.

3. Чистиков Д. В. Об одной характеристике деревьев, связанной с индивидуальным тестированием бесповторных функций // *Материалы XVIII Международной школы-семинара «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (Пенза, 28 сентября – 3 октября 2009 г.).* М.: Изд-во механико-математического ф-та МГУ, 2009. С. 94–99.

4. Бубнов С. Е., Вороненко А. А., Чистиков Д. В. Некоторые оценки длин тестов для бесповторных функций в базисе $\{\&, \vee\}$ // *Прикладная математика и информатика.* Вып. 33. М.: МАКС Пресс, 2009. С. 90–100. (Bubnov S. E., Voronenko A. A., Chistikov D. V. Some test length bounds for nonrepeating functions in the $\{\&, \vee\}$ basis // *Computational Mathematics and Modeling.* 2010. Vol. 21, № 2. P. 196–205.)

5. Чистиков Д. В. Тестирование бесповторных функций в различных базисах // *Сборник тезисов лучших дипломных работ 2010 года.* М.: Изд. отдел ф-та ВМК МГУ им. М. В. Ломоносова. 2010. С. 102–104.

6. Вороненко А. А., Чистиков Д. В. Расшифровка бесповторных функций оракулом — счетчиком четности // *Прикладная математика и информатика.* Вып. 34. М.: МАКС Пресс, 2010. С. 93–106. (Voronenko A. A., Chistikov D. V. Learning read-once functions using subcube parity queries // *Computational Mathematics and Modeling.* 2011. Vol. 22, № 1. P. 81–91.)

7. Чистиков Д. В. Бесповторные функции с труднотестируемыми подфункциями // *Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика.* 2010. № 4. С. 38–41.

8. Чистиков Д. В. Расшифровка бесповторных функций по двум младшим битам числа единиц подфункций // *Синтаксис и семантика логических систем: материалы 3-й Российской школы-семинара.* Иркутск: Изд-во Восточно-Сибирской государственной академии образования, 2010. С. 114–118.

9. Чистиков Д. В. О связи задач диагностического и проверяющего тестирования бесповторных функций // *Дискретная математика.* 2011. Т. 23, № 1. С. 46–50.

10. Чистиков Д. В. Бесповторные функции наименьшей тестовой сложности // *Сборник статей молодых ученых факультета ВМК МГУ.* Вып. 8. М.: Изд. отдел ф-та ВМК МГУ им. М. В. Ломоносова; МАКС Пресс, 2011. С. 135–144.

11. Вороненко А. А., Чистиков Д. В. Расшифровка бесповторных функций запросами тождественности // *Проблемы теоретической кибернетики. Материалы XVI Международной конференции (Нижний Новгород, 20–25 июня 2011 г.).* Нижний Новгород: Изд-во Нижегородского госуниверситета, 2011. С. 105–108.

12. Чистиков Д. В. Тестирование бесповторных функций в элементарном базисе // *Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика.* 2011. № 4. С. 37–40.

13. Chistikov D. V. Testing monotone read-once functions // Proc. of IWOCA 2011. *Lecture Notes in Computer Science.* Vol. 7056. Berlin; Heidelberg: Springer-Verlag, 2011. P. 121–134.