

На правах рукописи

ЗОЛОТЫХ Николай Юрьевич

**Расшифровка пороговых
и близких к ним функций**

01.01.09 – Дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
доктора физико-математических наук

Москва – 2013

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Нижегородский государственный университет им. Н. И. Лобачевского»

Научный консультант:

Шевченко Валерий Николаевич, доктор физико-математических наук, профессор, ФГБОУ ВПО «Нижегородский государственный университет им. Н. И. Лобачевского», заведующий кафедрой

Официальные оппоненты:

Леонтьев Владимир Константинович, доктор физико-математических наук, профессор, ФГБУН Вычислительный центр им. А. А. Дородницына РАН, главный научный сотрудник

Зуев Юрий Анатольевич, доктор физико-математических наук, профессор, ФГБОУ ВПО Московский государственный университет технологий и управления им. К. Г. Разумовского, профессор

Хачай Михаил Юрьевич, доктор физико-математических наук, доцент, ФГБУН Институт математики и механики им. Н. Н. Красовского УрО РАН, заведующий отделом

Ведущая организация:

ФГБУН Институт математики им. С. Л. Соболева СО РАН

Защита состоится 21 февраля 2014 г. в 11 час. 00 мин. на заседании диссертационного совета Д 501.001.44 при Московском государственном университете им. М. В. Ломоносова по адресу: 119991, ГСП-1, Москва, Ленинские горы, МГУ, 2-й учебный корпус, факультет ВМК, аудитория 685

С диссертацией можно ознакомиться в Фундаментальной библиотеке МГУ им. М. В. Ломоносова.

Автореферат разослан «_____» _____ г.

Ученый секретарь диссертационного совета

В. А. Костенко

Общая характеристика работы

Актуальность темы исследований. В целом ряде разделов математической кибернетики возникает задача восстановления (расшифровки) неизвестной дискретной функции из заданного класса с помощью последовательных вопросов о ее значении в точке. Требуется отыскать алгоритм расшифровки, использующий по возможности минимальное число вопросов о значении функции и приемлемое время для промежуточных вычислений.

Наиболее известной проблемой из этой серии является впервые рассмотренная В. К. Коробковым и Т. Л. Резником задача расшифровки монотонных булевых и многозначных функций [26, 27]. Известна сводимость к последней проблеме целого класса задач математической логики, математической экономики, целочисленного линейного программирования, теории распознавания образов.

В.Н.Шевченко рассмотрел задачу расшифровки пороговых функций k -значной логики [37–39]. Пороговые функции возникают во многих разделах математической кибернетики и дискретной математики и приложениях, например, в дискретной оптимизации [33, 39], распознавании образов [20, 21, 48], теории графов [19], при синтезе схем из функциональных элементов [29, 30, 32], нейронных сетей [42], в цифровой обработке сигналов [18, 50]. Их можно интерпретировать как характеристические функции подмножеств множества $\{0, 1, \dots, k - 1\}^n$, обладающих специальным свойством «линейной отделимости». В связи с последней возможностью естественно стремление расширить их область определения. Значительный интерес имеют постановки задач, в которых функции определены на множестве M целочисленных решений заданной системы линейных неравенств. Функция, отображающая M в множество $\{0, 1\}$, называется пороговой, если найдется гиперплоскость, разделяющая множества ее нулей и единиц (точек, в которых функция равна нулю или единице соответственно). К расшифровке таких функций сводятся специальные задачи теории распознавания образов с линейной разделяющей поверхностью. Большое значение задача расшифровки пороговых функций имеет в машинном обучении [48]. Другой смежной областью является связанная с большим кругом приложений теория тестов [28, 31, 34]. Таким образом, до-

статочным является целый ряд проблем, связанных с пороговыми функциями и их расшифровкой. Как правило, возникающие задачи — весьма сложные. Широко известной трудной проблемой, например, является оценка числа пороговых булевых функций. Для этой величины известна лишь установленная Ю. А. Зуевым [23] асимптотика ее логарифма. Асимптотика логарифма числа пороговых функций k -значной логики установлена А. А. Ирматовым и Ж. Д. Ковиянич [25]. Обстоятельный обзор результатов по пороговым булевым функциям и пороговым представлениям булевых функций содержится в [24].

Естественной мерой сложности алгоритма расшифровки является минимальное число вопросов, достаточное для расшифровки любой функции из заданного класса (*оракульная сложность*). Другой характеристикой является *вычислительная трудоемкость* — число операций, выполненных алгоритмом в худшем случае.

В. Н. Шевченко [38] предложил алгоритм расшифровки пороговой функции k -значной логики, имеющий при любом фиксированном n полиномиальные от $\log k$ оракульную сложность и вычислительную трудоемкость. Верхнюю оценку сложности алгоритма В. Н. Шевченко уточнил Т. Hegedüs [46], см. также [47]. В. Н. Шевченко [38] также показал, что полиномиального от n алгоритма, решающего данную задачу, не существует. Таким образом, для задачи расшифровки пороговой функции приведенные результаты заставляют ограничиться поиском алгоритмов, полиномиальных при фиксированном n . Для оценки их качества и для характеристики сложности всей задачи расшифровки пороговых функций необходимы результаты о близости предлагаемых алгоритмов к оптимальным. В частности, представляет интерес поиск нижних оценок сложности расшифровки, что приводит к исследованию структурных и мощностных свойств так называемого разрешающего множества [26] пороговой функции — такого множества точек из области определения M , значений функции в которых достаточно для однозначного восстановления функции в остальных точках. Дальнейшие результаты в этих направлениях означали бы более глубокое исследование структурных свойств и, возможно, мощностных характеристик класса пороговых функций.

До исследований автора нетривиальных нижних оценок сложности расшифровки пороговых функций (при фиксированном n и $k \rightarrow \infty$) известно не

было. М. Anthony, G. Brightwell, J. Shawe-Taylor [43] получили верхнюю оценку средней мощности минимального разрешающего множества пороговой функции. W. J. Bultman и W. Maass [44] исследовали сложность расшифровки пороговой функции, зависящей от двух переменных (использовалась несколько отличная терминология).

Цель работы заключается в построении эффективных алгоритмов расшифровки пороговых и близких к ним функций, определенных на множестве целочисленных решений заданной системы линейных неравенств; установлении нижних оценок сложности задачи расшифровки; анализе структурных и мощностных свойств минимального разрешающего множества пороговой функции. Особое внимание уделяется пороговым функциям k -значной логики, зависящих от n переменных.

Методы исследований. При построении алгоритмов расшифровки использовались результаты и методы целочисленного линейного программирования, теории систем линейных неравенств, теории чисел, комбинаторики. Некоторые алгоритмы используют и развивают подходы, предложенные В. Н. Шевченко при разработке им алгоритма расшифровки пороговых функций k -значной логики. При построении верхних и нижних оценок сложности расшифровки успешно применяются результаты о числе вершин выпуклой оболочки целочисленных решений систем линейных неравенств, полученные В. Н. Шевченко и его учениками [39]. Данный подход был применен и усовершенствован диссертантом для получения верхней оценки числа неприводимых точек политопа, что использовалось при построении неулучшаемой (по порядку при фиксированном n) верхней оценки мощности минимального разрешающего множества пороговой функции. Предложен новый подход, на основе которого получена нетривиальная нижняя оценка сложности расшифровки пороговой функции k -значной логики.

Научная новизна. Диссертация посвящена изучению задачи расшифровки пороговых и близких к ним функций, заданных на множестве целочисленных решений системы линейных неравенств (целых точек политопа). Особое внимание уделяется важному частному случаю — пороговым функциям k -значной логики. Все полученные результаты являются новыми и могут быть

кратко сформулированы следующим образом:

- 1) Разработан алгоритм расшифровки функций, заданных на множестве целочисленных точек политопа и обладающих свойством, что множества нулей и единиц каждой такой функции можно описать системами линейных неравенств. При любой фиксированной размерности n и некоторых дополнительных ограничениях алгоритм является полиномиальным от размера линейной системы, описывающей политоп.
- 2) Для пороговых функций, определенных на множестве целочисленных точек политопа, предложен алгоритм расшифровки, при фиксированной размерности полиномиальный от размера задания политопа. Установлена нижняя оценка сложности этой задачи. Оракульная сложность предложенного алгоритма при фиксированном n близка по порядку к нижней оценке сложности.
- 3) Для пороговых функций k -значной логики предложен алгоритм расшифровки, полиномиальный при фиксированном n . Установлена нижняя оценка сложности этой задачи. Оракульная сложность предложенного алгоритма при фиксированном n близка по порядку к нижней оценке сложности.
- 4) Описано строение минимального разрешающего множества пороговой функции k -значной логики. Найдены верхняя и нижняя оценка длины обучения в классе таких функций; при фиксированном n эти оценки совпадают по порядку.
- 5) Разработан алгоритм расшифровки пороговых функций k -значной логики, зависящих от двух переменных. Для этих функций установлен порядок сложности расшифровки, найдены точное значение длины обучения и асимптотическое значение средней мощности минимального разрешающего множества.
- 6) Установлена связь задачи расшифровки пороговой функции двух переменных с проблемой нахождения диофантовых приближений вещественных чисел. Предложен полиномиальный алгоритм приближения веще-

ственного числа, заданного оракулом, и полиномиальный алгоритм приближения алгебраического числа, заданного минимальным многочленом.

- 7) Предлагается новая модификация («графовый» тест проверки смежности экстремальных лучей) метода двойного описания построения вершинного описания полиэдра. Теоретическая оценка сложности построенной модификации и результаты экспериментов показали преимущество алгоритма по сравнению с классическим его вариантом.

Теоретическая и практическая значимость. Работа носит теоретический характер. Полученные в диссертации результаты могут быть использованы при дальнейших исследованиях пороговых функций, в частности, при изучении их структуры, числа, соотношения с другими близкими функциями и т. п. Диссертация имеет ценность для таких приложений, как дискретная оптимизация, распознавание образов, машинное обучение. Новая модификация метода двойного описания может использоваться в практических приложениях, где встречается задача построения общего решения системы линейных неравенств и двойственная к ней задача, например, в оптимизации, вычислительной физике, биоинформатике и др.

Результаты диссертации могут найти применение в исследованиях, проводимых в Московском государственном университете им. М. В. Ломоносова, Вычислительном центре им. А. А. Дородницына РАН, Институте прикладной математики им. М. В. Келдыша РАН, Институте математики им. С. Л. Соболева Сибирского отделения РАН, Нижегородском государственном университете им. Н. И. Лобачевского.

Апробация работы. Результаты диссертации докладывались и обсуждались на Международных семинарах «Дискретная математика и ее приложения» (Москва, 1995, 1998, 2001, 2004, 2007, 2012), на XVI Международной конференции «Проблемы теоретической кибернетики» (Нижний Новгород, 2011), на Международных конференциях «Математические алгоритмы» (Нижний Новгород, 1994, 1995), на Международной конференции «Алгебра и линейная оптимизация», посвященной 100-летию С. Н. Черникова (Екатеринбург, 2012) на Всероссийской конференции «Проблемы оптимизации и эко-

номические приложения» (Омск, 2006), на Всероссийской конференции «Математическое программирование и приложения» (Екатеринбург, 2007, 2011), на Российских конференциях «Дискретный анализ и исследование операций» (Новосибирск, 2004), «Дискретная оптимизация и исследование операций» (Алтай, 2010), на школе-семинаре «Синтез и сложность управляющих систем» (Нижний Новгород, 1994; Нижний Новгород, 2000; Пенза, 2002; Нижний Новгород, 2003), на Молодежной научной школе по дискретной математике и ее приложениям под руководством чл.-корр. РАН О. Б. Лупанова (Москва, 1997; Москва, 2000; Нижний Новгород, 2001), на заседаниях спецсеминара «Дискретная математика и математическая кибернетика» ВМК МГУ, Нижегородского семинара по дискретной математике.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения и списка литературы. Общий объем работы — 208 страниц. Список литературы содержит 167 наименований. В первой главе содержатся результаты о пороговых и близких к ним функциях, которые далее используются для построения алгоритмов расшифровки и установлении нижних оценок сложности. Во второй главе предлагаются алгоритмы расшифровки пороговых и близких к ним функций. Третья глава посвящена нижним оценкам сложности задачи расшифровки. В ней также описаны результаты о структурных и мощностных свойствах разрешающего множества пороговой функции. В четвертой главе устанавливается связь между задачей расшифровки пороговой функцией и задачей нахождения наилучшего диофантового приближения.

Публикации. По теме диссертации автором опубликовано 17 работ [1–17], из них 11 — в изданиях, рекомендованных ВАК [2, 3, 6, 8–10, 12–16]. Все основные результаты принадлежат автору. В работах, выполненных совместно с В. Н. Шевченко и А. Ю. Чирковым, диссертанту принадлежат формулировки и доказательства результатов, включенных в диссертацию. Диссертация продолжает исследования, начатые автором в его кандидатской диссертации [22].

Финансовая поддержка. Диссертация выполнена при финансовой поддержке РФФИ (гранты №№ 93-01-00491-а, 96-01-00639-а, 00-01-00599-а, 05-01-00552-а, 09-01-00545-а); ФЦП «Исследования и разработки по приоритет-

ным направлениям развития научно-технологического комплекса России на 2007–2013 годы», (государственный контракт № 11.519.11.4015); ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы (государственные контракты № 02.740.11.5131, № 14.В37.21.0393).

Краткое содержание и основные результаты

Во введении диссертации обосновывается актуальность темы, приводится обзор литературы и излагаются основные результаты.

Глава 1 посвящена изучению основных свойств пороговых и близких к ним функций, определенных в целочисленных точках политопа. В разделе 1.1 вводятся основные классы рассматриваемых функций и даются необходимые и достаточные условия принадлежности функций тому или иному из этих классов. Обозначим через $\mathfrak{P}(n, l, \gamma)$ множество выпуклых политопов $P \subseteq \mathbb{R}^n$, каждый из которых можно задать системой l линейных неравенств с целочисленными коэффициентами, ограниченными по абсолютной величине числом γ ; пусть $\mathfrak{M}(n, l, \gamma) = \{P \cap \mathbb{Z}^n : P \in \mathfrak{P}(n, l, \gamma)\}$. Для некоторых $n \geq 2$, $l > n$, $\gamma \geq 2$ рассмотрим множество $M \in \mathfrak{M}(n, l, \gamma)$; предположим, что $M \neq \emptyset$. Множество всех функций, отображающих M в $\{0, 1\}$, обозначим через $\mathfrak{F}(M)$. Пусть $E_k = \{0, \dots, k-1\}$. Класс $\mathfrak{F}(E_k^n)$ объединяет функции булевой логики, а $\mathfrak{F}(E_k^n)$ при $k \geq 2$ является подклассом тех функций k -значной логики, множество значений которых есть $\{0, 1\}$. Для $f \in \mathfrak{F}(M)$ обозначим через $M_0(f)$ и $M_1(f)$ множество нулей и единиц функции f соответственно, т. е. $M_\nu(f) = \{x \in M : f(x) = \nu\}$ ($\nu = 0, 1$). Обозначим через $N_\nu(f) = \text{Vert } M_\nu(f)$ множество вершин (крайних точек) политопа $\text{Conv } M_\nu(f)$ ($\nu = 0, 1$).

Для каждого $\nu \in \{0, 1\}$ обозначим через $\mathfrak{F}_\nu(M)$ множество таких функций $f \in \mathfrak{F}(M)$, для которых $M_\nu(f)$ можно описать в виде некоторой системы линейных неравенств $Ax \leq a_0$, т. е. $M_\nu(f) = \{x \in M : Ax \leq a_0\}$. Систему $Ax \leq a_0$ назовем *характеристической*. Обозначим через $m_\nu(f)$ наименьшее число неравенств в системе $Ax \leq a_0$, при котором возможно такое описание. Если для некоторого $\nu \in \{0, 1\}$ справедливо $f \in \mathfrak{F}_\nu(M)$ и $m_\nu(f) = 1$, то функция f называется *пороговой*. Пусть для такой f неравенство $\sum_{j=1}^n a_j x_j \leq a_0$, которое назовем *пороговым*, описывает множество $M_0(f)$. Можно считать, что $a_j \in \mathbb{Z}$

($j = 0, 1, \dots, n$). Обозначим через $\mathfrak{T}(M)$ множество всех пороговых функций, заданных на M .

В разделе 1.2 для функций из классов $\mathfrak{T}(M)$, $\mathfrak{F}_0(M)$, $\mathfrak{F}_1(M)$ получены верхние оценки величины коэффициентов характеристической системы, а в разделе 1.3 — верхние оценки величин $|N_\nu(f)|$ ($\nu = 0, 1$). Также в разделе 1.3 исследуется задача построения множеств $N_\nu(f)$ по заданной характеристической системе функции f .

Мощностные свойства классов $\mathfrak{T}(M)$, $\mathfrak{F}_0(M)$, $\mathfrak{F}_1(M)$ изучаются в разделе 1.4. Рассмотрим класс $\mathfrak{F}_\nu(M, m)$ ($\nu = 0, 1$) таких функций f из $\mathfrak{F}_\nu(M)$, для которых $m_\nu(f) = m$. Доказано, что при $\gamma \geq 1$, $m \geq 1$ справедлива асимптотическая оценка $\log |\mathfrak{F}_\nu(M, m)| \lesssim mn^3 \log(\gamma \sqrt{n})$ ($n \rightarrow \infty$). Отсюда для класса пороговых функций при $\gamma \geq 1$ получаем $\log |\mathfrak{T}(M)| \lesssim n^3 \log(\gamma \sqrt{n})$ ($n \rightarrow \infty$).

Соотношения между классами $\mathfrak{T}(M)$ и $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$ исследуются в разделе 1.5. В частности, построены примеры, показывающие, что если $k \geq 2$ и $n \geq 3$, то $\mathfrak{T}(E_k^n)$ является собственным подмножеством класса $\mathfrak{F}_0(E_k^n) \cap \mathfrak{F}_1(E_k^n)$. Приведено доказательство, что если $k \geq 3$, то $\mathfrak{T}(E_k^2) = \mathfrak{F}_0(E_k^2) \cap \mathfrak{F}_1(E_k^2)$ (данное утверждение приведено в [39, стр. 169] без доказательства).

Раздел 1.6 посвящен задаче построения вершин и экстремальных лучей полиэдра $P = \{x \in \mathbb{R}^n : Ax \leq a_0\}$, где $A \in \mathbb{Z}^{m \times n}$, $a_0 \in \mathbb{Z}^m$. Эта задача возникает как вспомогательная при построении алгоритмов расшифровки пороговых и близких к ним функций, но также появляется в большом числе других приложений и представляет несомненный самостоятельный интерес. Стандартным способом она сводится к построению экстремальных лучей полиэдрального (многогранного) конуса $\{(x, x_0) \in \mathbb{R}^{n+1} : Ax \leq x_0 a_0, x_0 \geq 0\}$. Для решения задачи известны различные методы, один из них — хорошо известный «метод двойного описания» [49] (другие распространенные названия — алгоритм Моцкина–Бургера [35] или алгоритм Фурье–Моцкина [40, 41]).

На каждой итерации алгоритм определяет множество всех пар смежных экстремальных лучей некоторого конуса $C = \{x \in \mathbb{R}^n : Ax \geq 0\}$, где $A \in \mathbb{Z}^{m \times n}$. Пусть U — множество экстремальных лучей конуса C , $|U| = s$. Обозначим $Z(u) = \{i : a_i u = 0\}$, где a_i — i -я строка матрицы A , $u \in U$. Хорошо известное «комбинаторное правило» [45] проверки смежности утверждает, что для смежности лучей u и v из U необходимо и достаточно, чтобы в U не существовало

луча w , отличного от u и v , такого, что $Z(u) \cap Z(v) \subseteq Z(w)$. Мы предлагаем следующую «графовую» модификацию комбинаторного теста. По конусу C построим простой граф G : множество вершин графа G есть множество U , а $\{u, v\}$ образует ребро в G тогда и только тогда, когда $|Z(u) \cap Z(v)| \geq n - 2$. Множество всех ребер графа G обозначим $E(G)$. Мы доказываем, что для того, чтобы лучи u и v из U были смежны необходимо и достаточно, чтобы в $U(C)$ не существовало луча w , отличного от u и v , такого, что $\{u, w\} \in E(G)$, $\{v, w\} \in E(G)$ и $Z(u) \cap Z(v) \subseteq Z(w)$. Трудоемкость построения всех пар экстремальных лучей по комбинаторному правилу составляет $O(ms^3)$, а по его «графовой» модификации $O(ms^2 + ms\delta^2)$, где δ равно максимуму из степеней вершин в графе G . Так как $\delta < s$, то трудоемкость «графового» теста всегда асимптотически не превосходит верхней оценки трудоемкости «комбинаторного». Во многих задачах $\delta \ll s$ и преимущество нового алгоритма более существенно. Результаты вычислительного эксперимента подтверждают это превосходство. Диссертантом предлагаются также другие модификации метода двойного описания.

Результаты первой главы диссертации опубликованы в работах [2, 8, 11].

В **главе 2** предлагаются алгоритмы расшифровки пороговых и близких к ним функций. Пусть каждая функция f из некоторого класса $\mathfrak{F}' \subseteq \mathfrak{F}(M)$ задана оракулом, позволяющим по произвольной точке $x \in M$ определить $f(x)$. Под *расшифровкой* функции из известного класса \mathfrak{F}' понимается задача, в которой по заданным $C \in \mathbb{Z}^{l \times n}$, $c_0 \in \mathbb{Z}^l$ и заданному оракулу функции $f \in \mathfrak{F}'$, где $M = \{x \in \mathbb{Z}^n : Cx \leq c_0\}$, необходимо найти такие точки $x^{(1)}, x^{(2)}, \dots, x^{(t)}$ из M , значений в которых достаточно для однозначного определения f в остальных точках из M .

Пусть \mathcal{A} — алгоритм расшифровки функции в классе \mathfrak{F}' . Предположим, что при расшифровке функции $f \in \mathfrak{F}'$ алгоритм \mathcal{A} обращается к оракулу в $\tau(\mathcal{A}, f)$ точках и выполняет $\rho(\mathcal{A}, f)$ операций. *Оракульной сложностью* алгоритма \mathcal{A} назовем величину

$$\tau_M(\mathcal{A}) = \max_{f \in \mathfrak{F}'} \tau(\mathcal{A}, f).$$

Вычислительной трудоемкостью алгоритма \mathcal{A} назовем число операций, вы-

полненных алгоритмом в худшем случае:

$$\rho_M(\mathcal{A}) = \max_{f \in \mathfrak{F}'} \rho(\mathcal{A}, f).$$

Пусть, как обычно, $M = \{x \in \mathbb{Z}^n : Cx \leq c_0\} \in \mathfrak{M}(n, l, \gamma)$, $C \in \mathbb{Z}^{l \times n}$, $c_0 \in \mathbb{Z}^l$, $|c_{ij}| \leq \gamma$, ($i = 1, 2, \dots, l$; $j = 0, 1, \dots, n$). Алгоритм \mathcal{A} назовем *полиномиальным*, если функция $\rho_M(\mathcal{A})$ ограничена некоторым полиномом от трех переменных $n, l, \log \gamma$. Будем говорить, что алгоритм \mathcal{A} полиномиален при фиксированной размерности n (*квазиполиномиален*), если найдется многочлен $p_n(\cdot, \cdot)$, степень и коэффициенты которого зависят только от n , такой, что $\rho_M(\mathcal{A}) \leq p_n(l, \log \gamma)$. Очевидно, $\tau_M(\mathcal{A}) \leq \rho_M(\mathcal{A})$ и поэтому верхняя оценка вычислительной трудоемкости алгоритма является таковой и для его оракульной сложности.

Если из контекста ясно, о каком множестве M идет речь, то вместо $\tau_M(\mathcal{A})$ и $\rho_M(\mathcal{A})$ будем писать соответственно $\tau(\mathcal{A})$ и $\rho(\mathcal{A})$.

Для классов $\mathfrak{T}(M)$, $\mathfrak{F}_0(M)$, $\mathfrak{F}_1(M)$, $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$ от алгоритмов расшифровки будем требовать, чтобы они возвращали также коэффициенты характеристических систем функции f . В случае пороговой функции — коэффициенты порогового неравенства.

В диссертации рассматриваются алгоритмы (условные тесты), в которых выбор точки для нового обращения к оракулу, определяется ответами на предыдущие вопросы. Что же касается алгоритмов, не учитывающих ответы на предыдущие вопросы (безусловные тесты), то для рассматриваемых классов они оказываются весьма неэффективными. Множество $U \subseteq M$ называется *безусловным тестом* для класса функций \mathfrak{F}' , если для любых двух f, g из \mathfrak{F}' , $f \neq g$, найдется точка $x \in U$, такая, что $f(x) \neq g(x)$. В разделе 2.2 показано, что классы $\mathfrak{T}(M)$, $\mathfrak{F}_0(M)$, $\mathfrak{F}_1(M)$, $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$ обладают единственным безусловным тестом $U = M$.

В разделе 2.3 рассматривается задача расшифровки в $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$. Вначале (в подразделе 2.3.1) строится вспомогательный оракульный алгоритм $\mathcal{A}_{\text{опт}}$, решающий задачу максимизации линейной функции на множестве $M_\nu(f)$, где $f \in \mathfrak{F}_{1-\nu}(M)$. Алгоритм $\mathcal{A}_{\text{опт}}$ для любого $\nu \in \{0, 1\}$, любой заданной оракулом функции $f \in \mathfrak{F}_{1-\nu}(M)$ и любого вектора $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$ находит

точку $p = (p_1, \dots, p_n) \in M_v(f)$, такую, что

$$\sum_{j=1}^n a_j p_j = \max \left\{ \sum_{j=1}^n a_j x_j : (x_1, \dots, x_n) \in M_v(f) \right\},$$

или устанавливает, что $M_v(f) = \emptyset$. При фиксированном n алгоритм имеет полиномиальную от l и $\log \alpha$ вычислительную трудоемкость и совершает не более $n^{10n-1} l^{\lfloor \frac{n}{2} \rfloor} \log^n(\alpha + 1)$ (при $n \geq 2$) и не более $8 + 2 \log \gamma$ (при $n = 1$) обращений к оракулу, где $\alpha = \max\{\gamma, |a_j|, j = 1, \dots, n\}$.

В подразделе 2.3.2 предлагается алгоритм \mathcal{A}_0 расшифровки в классе $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$. Обозначим через $\mathfrak{F}(M, h)$ множество таких функций $f \in \mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$, для которых $\min\{m_0(f), m_1(f)\} \leq h$. В классе $\mathfrak{F}(M, h)$, где $M \in \mathfrak{M}(n, l, \gamma)$, при любом фиксированном n алгоритм имеет полиномиальную от h, l и $\log \gamma$ вычислительную трудоемкость $\rho(\mathcal{A}_0)$ и оракульную сложность

$$\tau(\mathcal{A}_0) = O\left((l + h)^{\lfloor \frac{n}{2} \rfloor^2} l^{\lfloor \frac{n}{2} \rfloor} \log^{(n-1)\lfloor \frac{n}{2} \rfloor + n}(\gamma + 1)\right)$$

(асимптотика при фиксированном n).

Очевидно, алгоритм \mathcal{A}_0 применим и для расшифровки функций из класса $\mathfrak{T}(M)$. Для последнего случая однако существует более эффективный алгоритм \mathcal{A}_1 , описанный в разделе 2.4. Вначале (в подразделе 2.4.1) строится вспомогательный алгоритм \mathcal{A}_1^+ . Обозначим через $\mathfrak{T}_+(M)$ множество тех функций из $\mathfrak{T}(M)$, для которых существует пороговое неравенство с коэффициентом $a_0 > 0$. Алгоритм \mathcal{A}_1^+ проводит расшифровку при допущении $f \in \mathfrak{T}_+(M)$. На его основе в разделе 2.4.2 построен алгоритм \mathcal{A}_1 расшифровки в классе $\mathfrak{T}(M)$, для которого при фиксированном n величина $\rho(\mathcal{A}_1)$ ограничена полиномом от l и $\log \gamma$ и

$$\tau(\mathcal{A}_1) \leq 16n^{10n-1} l^{\lfloor \frac{n}{2} \rfloor} \log^n(\gamma + 1) = O\left(l^{\lfloor \frac{n}{2} \rfloor} \log^n(\gamma + 1)\right).$$

(асимптотика при фиксированном n). В классе $\mathfrak{T}(E_k^n)$ при любом фиксированном n алгоритм имеет оракульную сложность

$$\tau(\mathcal{A}_1) = O(\log^n k).$$

В разделе 2.5 для расшифровки функций из класса $\mathfrak{T}(E_k^2)$ удалось построить более эффективный алгоритм \mathcal{A}_2 . Алгоритм \mathcal{A}_2 имеет полиномиальную

вычислительную трудоемкость и оракульную сложность

$$\tau(\mathcal{A}_2) \leq 6 \log(k - 1) + 4.$$

В разделе 2.6 исследуется задача расшифровки пороговой функции, заданной более информативным — «расширенным» — оракулом, который в отличие от «обычного» оракула принимает на вход произвольные точки из \mathbb{Q}^n , а не только из M . Расширенный оракул связан с конкретным пороговым неравенством функции f . По заданной точке $x \in \mathbb{Q}^n$ он возвращает 0, если пороговое неравенство выполнено, и 1 в противном случае. Под *расшифровкой пороговой функции f , заданной с помощью расширенного оракула*, будем понимать процедуру восстановления коэффициентов ее любого возможного порогового неравенства с помощью обращений к этому оракулу. Предложен алгоритм \mathcal{A}_{ext} расшифровки функции из класса $\mathfrak{T}(E_k^n)$, заданной с помощью расширенного оракула, для которого вычислительная трудоемкость $\rho(\mathcal{A}_{\text{ext}})$ при фиксированном n ограничена полиномом от $\log k$, а для оракульной сложности справедливо

$$\rho(\mathcal{A}_{\text{ext}}) = \frac{n^4}{2} \log(n + 1) + 2n^3 \log k \quad (n \rightarrow \infty, \quad k \rightarrow \infty).$$

Результаты второй главы опубликованы в [1, 2, 4, 9, 12, 16].

В **главе 3** устанавливаются нижние оценки сложности расшифровки пороговых функций. Под *сложностью расшифровки* в некотором классе $\mathfrak{F}' \subseteq \mathfrak{F}(M)$ понимается величина

$$\tau(\mathfrak{F}') = \min_{\mathcal{A}} \tau(\mathcal{A}) = \min_{\mathcal{A}} \max_{f \in \mathfrak{F}'} \tau(\mathcal{A}, f),$$

где минимум берется по всем алгоритмам \mathcal{A} расшифровки в классе \mathfrak{F}' . Множество $T \subseteq M$ называется *разрешающим* для f в классе \mathfrak{F}' , если для любой функции $g \in \mathfrak{F}'$, $f \neq g$, найдется по крайней мере одна точка $z \in T$, такая, что $g(z) \neq f(z)$. Разрешающее множество, никакое собственное подмножество которого не является разрешающим для f , называется *минимальным* или *ту-пиковым*. Разрешающее множество минимальной мощности называется *наименьшим*. Его мощность обозначим через $\sigma(\mathfrak{F}', f)$. *Длиной обучения* назовем величину

$$\sigma(\mathfrak{F}') = \max_{f \in \mathfrak{F}'} \sigma(\mathfrak{F}', f) = \max_{f \in \mathfrak{F}'} \min_{\mathcal{A}} \tau(\mathcal{A}, f).$$

Справедливы неравенства $\tau(\mathfrak{F}') \geq \sigma(\mathfrak{F}')$, $\tau(\mathfrak{F}') \geq \log |\mathfrak{F}'|$, являющиеся ключевыми для получения в диссертации нижних оценок сложности расшифровки. Средней мощностью минимального разрешающего множества в классе \mathfrak{F}' называется

$$\bar{\sigma}(\mathfrak{F}') = \frac{1}{|\mathfrak{F}'|} \sum_{f \in \mathfrak{F}'} \sigma(\mathfrak{F}', f).$$

Для класса пороговых функций $\mathfrak{I}(M)$ будем использовать следующие сокращенные обозначения:

$$\tau(M) = \tau(\mathfrak{I}(M)), \quad \sigma(M) = \sigma(\mathfrak{I}(M)), \quad \bar{\sigma}(M) = \bar{\sigma}(\mathfrak{I}(M)).$$

В разделе 3.2 получены некоторые вспомогательные результаты о строении конуса $K(f)$ разделяющих функционалов функции $f \in \mathfrak{I}(M)$. $K(f)$ описывается следующей системой линейных неравенств относительно переменных a_0, a_1, \dots, a_{n+1} :

$$\left\{ \begin{array}{l} \sum_{j=1}^n a_j x_j \leq a_0 \quad \text{для всех } (x_1, \dots, x_n) \in M_0(f); \\ \sum_{j=1}^n a_j x_j \geq a_0 + a_{n+1} \quad \text{для всех } (x_1, \dots, x_n) \in M_1(f); \\ a_{n+1} \geq 0. \end{array} \right.$$

Показано, что конус $K(f)$ полномерный (телесный) и в важном случае $\text{Affdim } M = n$ — острый. Из теории линейных неравенств выводится лемма о двойственном описании конуса $K(f)$. В частности, если $\text{Affdim } M = n$, то $K(f)$ имеет единственное с точностью до положительных множителей минимальное порождающее множество (остов)

$$\left\{ \widetilde{b}^{(i)} = (b_0^{(i)}, b_1^{(i)}, \dots, b_n^{(i)}, b_{n+1}^{(i)}), \quad i = 1, \dots, s \right\}.$$

В разделе 3.3 исследуется структура разрешающего множества пороговой функции. Множество $T = T_0 \cup T_1$, $T_\nu \subseteq M_\nu(f)$ ($\nu = 0, 1$) является разрешающим для $f \in \mathfrak{I}(M)$ тогда и только тогда, когда система неравенств

$$\left\{ \begin{array}{l} \sum_{j=1}^n a_j x_j \leq a_0 \quad \text{для всех } (x_1, \dots, x_n) \in T; \\ \sum_{j=1}^n a_j x_j \geq a_0 + a_{n+1} \quad \text{для всех } (x_1, \dots, x_n) \in T; \\ a_{n+1} \geq 0. \end{array} \right.$$

описывает конус $K(f)$. Отсюда, в частности, получаем единственность минимального разрешающего множества функции $f \in \mathfrak{T}(M)$ (это обобщение известного результата о булевых пороговых функциях). Обозначим его через $T(f) = T_0(f) \cup T_1(f)$, $T_\nu(f) \subseteq M_\nu(f)$ ($\nu = 0, 1$). Имеем также $N_\nu(f) \subseteq T_\nu(f)$ ($\nu = 0, 1$) (это обобщение результата [39]).

Пусть $\text{Affdim } M = n$ и $f \in \mathfrak{T}(M)$. Не нарушая общности, будем считать, что в остове конуса $K(f)$ компонента $b_{n+1}^{(i)} > 0$ ($i = 1, \dots, \mu$) и $b_{n+1}^{(i)} = 0$ ($i = \mu + 1, \dots, s$). Пусть $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$,

$$M_0(f, a) = \left\{ (y_1, \dots, y_n) \in M : \sum_{j=1}^n a_j y_j = \max_{x \in M_0(f)} \sum_{j=1}^n a_j x_j \right\},$$

$$M_1(f, a) = \left\{ (y_1, \dots, y_n) \in M : \sum_{j=1}^n a_j y_j = \min_{x \in M_1(f)} \sum_{j=1}^n a_j x_j \right\}.$$

Обозначим через $N_\nu(f, a)$ множество крайних точек (вершин) выпуклой оболочки множества $M_\nu(f, a)$. Доказано, что если $\text{Affdim } M = n$, тогда для любой функции $f \in \mathfrak{T}(M)$

$$T(f) = \bigcup_{i=1}^{\mu} \left(N_0(f, \widetilde{b}^{(i)}) \cup N_1(f, \widetilde{b}^{(i)}) \right) = \bigcup_a \left(N_0(f, a) \cup N_1(f, a) \right),$$

в последнем случае объединение берется по всем $a = (a_1, a_2, \dots, a_n) \in \mathbb{Z}^n$ таким, что неравенство

$$\sum_{j=1}^n a_j x_j \leq \max_{x \in M_0(f)} \sum_{j=1}^n a_j x_j$$

является пороговым для функции f .

В разделе 3.4 на основе анализа структуры разрешающего множества, проведенного ранее, выводятся нижние оценки длины обучения в классе $\mathfrak{T}(M)$. Доказано, что для любых $n \geq 2$ и $l > n$ найдется такое γ_0 , что для всех $\gamma \geq \gamma_0$ существует политоп $P \in \mathfrak{P}(n, l, \gamma)$ такой, что при фиксированном n

$$\tau(M) \geq \sigma(M) = \Omega(l^{\lfloor n/2 \rfloor} \log^{n-1} \gamma),$$

где $M = P \cap \mathbb{Z}^n$. Для класса пороговых функций k -значной логики установлена оценка при фиксированном n

$$\tau(E_k^n) \geq \sigma(E_k^n) \geq \frac{\left(\frac{1}{2} \log k - n - 3 - (n-1) \log(n-2) \right)^{n-2}}{4(n-1)3^{n-1}(n-2)^{n-2}((n-2)!)^2} = \Omega(\log^{n-2} k).$$

В разделе 3.5 предлагается другая характеристика минимального разрешающего множества $T(f)$ пороговой функции $f \in \mathfrak{T}(M)$. Пусть $Q(f) = \text{Cone}(M_0(f) - M_1(f))$; если f — тождественная константа, то $Q(f)$ — нулевой конус;

$$R_0(f) = \text{Conv}(M_0(f)) + Q(f), \quad R_1(f) = \text{Conv}(M_1(f)) - Q(f).$$

Доказано, что если $f \in \mathfrak{T}(M)$, то

$$T_\nu(f) = \text{Vert } R_\nu(f) \quad (\nu = 0, 1).$$

Отсюда получаем, что если $x, y \in T_\nu(f)$ ($\nu = 0, 1$) и $x \neq y$, то

$$2x - y \notin R_0(f) \cup R_1(f) \quad (0.1).$$

В общем случае удобного описания множеств $R_\nu(f)$ ($\nu = 0, 1$), которое позволило бы достаточно точно оценить $|\text{Vert } R_\nu(f)|$, не найдено. Тем не менее, в разделе 3.6 такое описание получено для подкласса $\mathfrak{T}'(E_k^n)$ таких пороговых функций f , для каждой из которых найдется пороговое неравенство, в котором $a_0 \in \mathbb{Z}$, $a_j \in \mathbb{Z}$, $0 < a_0 < a_j(k-1)$ ($j = 1, 2, \dots, n$).

Говорят, что множество $G \subset \mathbb{Z}_+^n$ обладает *свойством разделенности*, если из условий $x, y \in G$ и $x \neq y$ следует $2x - y \notin \mathbb{Z}_+^n$ [36]. Если $f \in \mathfrak{T}'(E_k^n)$, то из (0.1) получаем, что каждое из множеств $T_0(f)$ и $T_1(f)$ обладает свойством разделенности. Далее для получения верхних оценок $|T_0(f)|$ и $|T_1(f)|$ используется подход [36, 39]. Доказано, что для любой функции $f \in \mathfrak{T}'(E_k^n)$ при $n \geq 2$

$$|T_\nu(f)| \leq n(1 + \log n) \left(1 + \log(k+1)\right)^{n-2} \quad (\nu = 0, 1).$$

В разделе 3.7 получены верхние оценки количества неприводимых точек в полиэдре (далее, в разделе 3.8, эти оценки используются для получения верхней оценки $\sigma(E_k^n) = O(\log^{n-2} k)$ при фиксированном $n \geq 2$). Пусть P — полиэдр в \mathbb{R}^n . Точка $x \in P \in \mathbb{Z}^n$ называется *неприводимой* в P (а, точнее, в $P \cap \mathbb{Z}^n$), если x нельзя представить в виде $x = \frac{1}{2}(y + z)$ ни для каких двух различных y и z из $P \cap \mathbb{Z}^n$. Пусть P, P_1, P_2, \dots, P_s — политопа в \mathbb{R}^n . Если $P = \bigcup_{i=1}^s P_i$, то $\{P_1, P_2, \dots, P_s\}$ называется *покрытием* политопа P . Если пересечение любых двух политопов в покрытии либо пусто, либо является их общей

гранью, то покрытие называется *правильным разбиением*. Если все политопы в правильном разбиении — симплексы, то разбиение называется *триангуляцией*. Основная идея получения верхней оценки числа неприводимых точек в политопе заключается в следующем. В подразделе 3.7.1 получена оценка количества неприводимых точек в параллелепипеде. В подразделе 3.7.2 показано, как для произвольного политопа P построить его покрытие параллелепипедами P_1, P_2, \dots, P_s . Для этого сначала строится триангуляция политопа, а затем каждый симплекс триангуляции покрывается параллелепипедами. Легко видеть, что любая неприводимая в $P \cap \mathbb{Z}^n$ точка x неприводима и в $P_i \cap \mathbb{Z}^n$ для любого i , если $x \in P_i$. Это свойство позволяет в подразделе 3.7.3 оценить количество неприводимых точек в P . А именно, доказано, что если P можно задать системой m линейных неравенств и $P \cap \mathbb{Z}^n \subseteq E_k^n$, то количество неприводимых в $P \cap \mathbb{Z}^n$ точек есть $O(m^{\lfloor \frac{n}{2} \rfloor} \log^{n-1} k)$. Заметим, что полученная оценка представляет самостоятельный интерес. В разделе 3.8 она используется для получения неулучшаемой верхней оценки длины обучения в классе пороговых функций.

В разделе 3.8, используя результаты разделов 3.6 и 3.7, мы показываем, что

$$\sigma(E_k^n) = O(\log^{n-2} k) \quad (k \rightarrow \infty).$$

Объединяя нижнюю и верхнюю оценки длины обучения, получаем, что при фиксированном $n \geq 2$

$$\sigma(E_k^n) = \Theta(\log^{n-2} k) \quad (k \rightarrow \infty).$$

В разделе 3.9 изучается задача построения минимального разрешающего множества пороговой функции $f \in \mathfrak{T}(M)$, $M = P \cap \mathbb{Z}^n$, по известным коэффициентам порогового неравенства и по известной системе, описывающей политоп P . Для решения этой задачи предлагается полиномиальная от $\log \gamma$ и l процедура (n фиксировано). Показано, как изменить алгоритм \mathcal{A}_1 , чтобы сложность нового алгоритма \mathcal{A}_1^o отличалась бы от сложности оптимального (по числу обращений к оракулу в худшем случае) алгоритма расшифровки не более, чем в $O(n^3 \log(n\gamma))$ раз. Для класса $\mathfrak{T}(E_k^n)$ сложность алгоритма \mathcal{A}_1^o отличается от сложности оптимального алгоритма не более, чем в $O(n^2 \log(nk))$ раз и при фиксированном n

$$\tau(E_k^n) \leq \tau(\mathcal{A}_1^o) = O(\log^{n-1} k).$$

В разделе 3.10 рассматривается случай пороговых функций двух переменных. Из результатов предыдущих разделов вытекает

$$4 \log k \lesssim \tau(E_k^2) \lesssim 6 \log k.$$

Для длины обучения в классе $\mathfrak{T}(E_k^2)$ в подразделе 3.10.1 установлено точное значение

$$\sigma(E_k^2) = 4.$$

В подразделе 3.10.2 получена асимптотика среднего значения мощности минимального разрешающего множества в классе $\mathfrak{T}(E_k^2)$:

$$\bar{\sigma}(E_k^2) = \frac{7}{2} + O\left(\frac{1}{k}\right).$$

В подразделе 3.10.3 получены следствия из этих результатов, касающиеся специальных разбиений плоскости прямыми.

Пороговые булевы функции рассматриваются в разделе 3.11. Справедливо следующее равенство: $\sigma(E_2^n) = \tau(E_2^n) = |E_2^n| = 2^n$. В данном разделе также показано, что сложность расшифровки в классе пороговых монотонных булевых функций совпадает со сложностью расшифровки в классе монотонных булевых функций.

В разделе 3.12 полученные результаты о верхних и нижних оценках сложности расшифровки применяются к анализу оракульной сложности задачи о рюкзаке.

Результаты третьей главы диссертации опубликованы в работах [3, 5–7, 10, 11, 14, 15, 17].

В **главе 4** показана связь задачи расшифровки пороговой функции двух переменных с проблемой нахождения диофантовых приближений вещественных чисел. Рассмотрим следующую задачу. Для $\alpha \in \mathbb{R}$, $\alpha \geq 0$, $Q \in \mathbb{N}$ требуется среди всех рациональных дробей со знаменателем, не превосходящим Q , найти наилучшее приближение $\frac{p}{q}$ к α :

$$\left| \alpha - \frac{p}{q} \right| = \min \left\{ \left| \alpha - \frac{y}{x} \right| : x \in \mathbb{N}, x \leq Q, y \in \mathbb{Z} \right\}.$$

Предположим, что вещественное число α задано оракулом, позволяющим по произвольному $r \in \mathbb{Q}$ определить, выполняется или нет неравенство $\alpha \leq r$.

В разделе 4.2 показано, как использовать алгоритм \mathcal{A}_2 для решения задачи наилучшего приближения к заданному таким образом числу. Время работы построенной процедуры ограничено полиномом от $\log k$, где $k = \max \{Q, \lceil \alpha Q \rceil\}$. В разделе 4.3 на основе полученных результатов строится полиномиальный алгоритм нахождения наилучших приближений алгебраических вещественных чисел, заданных минимальным многочленом.

Результаты четвертой главы диссертации опубликованы в работе [13].

В заключении обсуждаются основные результаты диссертации

Список публикаций

1. *Золотых Н. Ю.* Алгоритм расшифровки пороговой функции k -значной логики на плоскости с числом обращений к оракулу $O(\log k)$ // Труды Первой Международной конференции «Математические алгоритмы». — Н. Новгород: Издательство Нижегород. гос. ун-та, 1995. — С. 21–26.
2. *Золотых Н. Ю.* О пороговых и близких к ним функциях, определенных в целочисленных точках политопа // Дискретный анализ и исследование операций. Серия 1. — 1998. — Т. 5, № 2. — С. 40–54.
3. *Золотых Н. Ю.* Оракульная сложность задачи о рюкзаке // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Математическое моделирование и оптимальное управление. — 2000. — № 1. — С. 84–87.
4. *Золотых Н. Ю.* Пороговые функции, зависящие от двух переменных: сложность расшифровки и мощность разрешающего множества // Материалы четвертой молодежной научной школы по дискретной математике и ее приложениям. — М.: Издательство механико-матем. факультета МГУ, 2000. — С. 48–54.
5. *Золотых Н. Ю.* О сложности расшифровки пороговых функций, зависящих от двух переменных // Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем». Часть I. — М.: Издательство Центра прикладных исследований при механико-математическом ф-те МГУ, 2001. — С. 74–79.

6. *Золотых Н. Ю.* О сложности решения одного класса задач целочисленного линейного программирования // Дискретный анализ и исследование операций. Серия 2. — 2003. — Т. 10, № 1. — С. 3–10.
7. *Золотых Н. Ю.* Оценки мощности минимального разрешающего множества пороговой функции многозначной логики // Математические вопросы кибернетики. Вып. 17. — М.: Физматлит, 2008. — С. 159–168.
8. *Золотых Н. Ю.* Новая модификация метода двойного описания для построения остова многогранного конуса // Журнал вычислительной математики и математической физики. — 2012. — Т. 52, № 1. — С. 153–163.
9. *Золотых Н. Ю.* Расшифровка пороговой функции, заданной расширенным оракулом // Вестник Нижегородского университета им. Н.И. Лобачевского. — 2012. — № 3. — С. 175–178.
10. *Золотых Н. Ю., Чирков А. Ю.* О верхней оценке мощности минимального разрешающего множества пороговой функции // Дискретный анализ и исследование операций. — 2012. — Т. 19, № 5. — С. 35–46.
11. *Золотых Н. Ю., Чирков А. Ю.* Сложность расшифровки пороговых функций многозначной логики // Материалы XI Международного семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О. Б. Лупанова (18–23 июня 2012 г.). — М.: Издательство механико-матем. факультета МГУ, 2012. — С. 63–77.
12. *Золотых Н. Ю., Шевченко В. Н.* Расшифровка пороговых функций k -значной логики // Дискретный анализ и исследование операций. — 1995. — Т. 2, № 3. — С. 18–23.
13. *Золотых Н. Ю., Шевченко В. Н.* Расшифровка пороговых функций и диофантовы приближения // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Математическое моделирование и оптимальное управление. — 1998. — № 1. — С. 199–207.
14. *Золотых Н. Ю., Шевченко В. Н.* Об оценке сложности расшифровки поро-

говых функций k -значной логики // Журнал вычислительной математики и математической физики. — 1999. — Т. 39, № 2. — С. 346–352.

15. Шевченко В. Н., Золотых Н. Ю. О сложности расшифровки пороговых функций k -значной логики // Доклады РАН. — 1998. — Т. 362, № 5. — С. 606–608.
16. Shevchenko V. N., Zolotykh N. Y. Decoding of threshold functions defined on the integer points of a polytope // Pattern recognition and image analysis. — 1997. — V. 7, N. 2. — P. 235–240.
17. Shevchenko V. N., Zolotykh N. Y. Lower bounds for the complexity of learning half-spaces with membership queries // Lecture Notes in Computer Science. V. 1501. — Springer-Verlag, 1998. — P. 61–71.

Цитированная литература

18. *Архангельский С. В.* Информационный анализ цифровых сигналов. — Самара: Издательство Саратовского университета, Самарский филиал, 1991.
19. *Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И.* Лекции по теории графов. — М.: Наука, 1990.
20. *Журавлев Ю. И.* Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики. Вып. 33. — М.: Наука, 1978. — С. 5–68.
21. *Загоруйко Н. Г.* Прикладные методы анализа данных и знаний. — Новосибирск: ИМ СО РАН, 1999.
22. *Золотых Н. Ю.* Расшифровка пороговых и близких к ним функций многозначной логики: Дис. . . . канд. физ.-матем. наук / Нижегородский гос. университет им. Н. И. Лобачевского. — Нижний Новгород, 1998.
23. *Зуев Ю. А.* Асимптотика логарифма числа пороговых функций алгебры логики // Доклады АН СССР. — 1989. — Т. 306, № 3. — С. 528–530.
24. *Зуев Ю. А.* Пороговые функции и пороговые представления булевых функций // Математические вопросы кибернетики. Вып. 5. — М.: Физматлит, 1994. — С. 5–61.
25. *Ирматов А. А., Ковиянич Ж. Д.* Об асимптотике логарифма числа пороговых функций k -значной логики // Дискретная математика. — 1998. — Т. 10, № 3. — С. 35–56.
26. *Коробков В. К.* Оценка числа монотонных функций алгебры логики и сложности алгоритма отыскания разрешающего множества для произвольной монотонной функции алгебры логики // Доклады Академии Наук СССР. — 1963. — Т. 150, № 4. — С. 744–747.
27. *Коробков В. К., Резник Т. Л.* О некоторых алгоритмах вычисления монотонных функций алгебры логики // Доклады Академии Наук СССР. — 1962. — Т. 147, № 5. — С. 1022–1025.

28. *Кудрявцев В. Б.* Теория тестового распознавания // Дискретная математика. — 2006. — Т. 18, № 3. — С. 3–34.
29. *Лупанов О. Б.* О возможности синтеза схем из произвольных элементов // Труды математического института им. В. А. Стеклова. Т. 51. — М.: АН СССР, 1958. — С. 158–173.
30. *Лупанов О. Б.* О синтезе схем из пороговых элементов // Проблемы кибернетики. Вып. 26. — М.: Наука, 1973. — С. 109–140.
31. *Мошков М. Ю.* Условные тесты // Проблемы кибернетики. Вып. 40. — М.: Наука, 1983. — С. 131–170.
32. *Нечипорук Э. И.* О синтезе схем из пороговых элементов // Проблемы кибернетики. Вып. 11. — М.: Наука, 1964. — С. 49–62.
33. *Схрейвер А.* Теория линейного и целочисленного программирования. В 2-х тт. — М.: Мир, 1991.
34. *Чегис И. А., Яблонский С. В.* Логические способы контроля работы электрических схем // Труды Матем. Института АН СССР. — 1958. — Т. 51. — С. 270–360.
35. *Черников С. Н.* Линейные неравенства. — М.: Наука, 1968.
36. *Шевченко В. Н.* О числе крайних точек в целочисленном программировании // Кибернетика. — 1981. — № 2. — С. 133–134.
37. *Шевченко В. Н.* О некоторых функциях многозначной логики, связанных с целочисленным программированием // Методы дискретного анализа в теории графов и схем. Вып. 42. — Новосибирск: Институт матем. СО АН СССР, 1985. — С. 99–108.
38. *Шевченко В. Н.* О расшифровке пороговых функции многозначной логики // Комбинаторно–алгебраические методы в прикладной математике. — Горький: Издательство Горьковского университета, 1987. — С. 155–163.

39. *Шевченко В. Н.* Качественные вопросы целочисленного программирования. — М.: Физматлит, 1995.
40. *Шевченко В. Н.* Триангуляции выпуклых многогранников и их булевы функции // Математические вопросы кибернетики. Вып. 16. — М.: Физматлит, 2007. — С. 43–56.
41. *Шевченко В. Н., Груздев Д. В.* Модификация алгоритма Фурье–Моцкина для построения триангуляций // Дискретный анализ и исследование операций. Серия 2. — 2003. — Т. 10, № 10. — С. 53–64.
42. *Anthony M., Bartlett P. L.* Neural network learning: theoretical foundations. — Cambridge: Cambridge University Press, 1999.
43. *Anthony M., Brightwell G., Shawe-Taylor J.* On specifying boolean functions by labelled examples // Discrete Applied Mathematics. — 1995. — V. 61, N. 1. — P. 1–25.
44. *Bultman W. J., Maass W.* Fast identification of geometric objects with membership queries // Information and Computation. — 1995. — V. 118, N. 1. — P. 48–64.
45. *Burger E.* Über homogene lineare Ungleichungssysteme // Zeitschrift für Angewandte Mathematik und Mechanik. — 1956. — V. 36, N. 3/4. — P. 135–139.
46. *Hegedüs T.* Geometrical concept learning and convex polytopes // Proc. 7 annual conf. on Computational learning theory (COLT'94). — New York: ACM Press, 1994. — P. 228–236.
47. *Hegedüs T.* Generalized teaching dimensions and the query complexity of learning // Proc. 8 annual conf. on Computational learning theory (COLT'95). — New York: ACM Press, 1995. — P. 108–117.
48. *Mitchell T.* Machine Learning. — McGraw-Hill Science/Engineering/Math, 1997.
49. *Motzkin T., Raiffa H., Thompson G., Thrall R.* The double description method // Contributions to Theory of Games / Ed. by H. Kuhn, A.W.Tucker. — Princeton,

RI: Princeton University Press, 1953. — V. 2. — P. 51–73. — [Рус. пер.: *Моцкин Т. С., Райфа Х., Томпсон Дж. Л., Тролл Р. М.* Метод двойного описания // Матричные игры / Под ред. Н. Н. Воробьева. — М.: Физматгиз, 1961].

50. *Widrow B., Lehr M. A.* Adaptive signal processing. — Englewood-Cliffs, N. J.: Prentice-Hall, 1985.