

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

Объект авторского права  
УДК 519.65

**БУРДЕЛЁВ**  
**Александр Владимирович**

**Пороговые  $k$ -значные функции, их характеристика и применение в  
системах защиты информации**

**Автореферат**  
диссертации на соискание ученой степени  
кандидата физико-математических наук  
по специальности  
05.13.19 «Методы и системы защиты информации,  
информационная безопасность»

Минск – 2025

Научная работа выполнена в Белорусском государственном университете и Федеральном государственном казенном научном учреждении «Академия криптографии Российской Федерации»

Научный руководитель

**Никонов Владимир Глебович,**

доктор технических наук, профессор, член-корреспондент Академии криптографии Российской Федерации, ведущий научный сотрудник лаборатории №5 Научно-исследовательского центра Академии криптографии Российской Федерации

Официальные оппоненты:

**Тузиков Александр Васильевич,**

доктор физико-математических наук, профессор, член-корреспондент НАН Беларуси, заведующий лабораторией ГНУ «Объединенный институт проблем информатики НАН Беларуси»

**Волошко Валерий Анатольевич,**

кандидат физико-математических наук, заведующий сектором учреждения БГУ «Научно-исследовательский институт прикладных проблем математики и информатики»

Оппонирующая  
организация

**ГНУ «Институт математики Национальной академии наук Беларуси»**

Защита состоится 6 марта 2025 года в 14:30 на заседании совета по защите диссертаций Д 02.01.02 при Белорусском государственном университете по адресу: 220030, Республика Беларусь, г. Минск, ул. Ленинградская, 8 (корпус юридического факультета), ауд. 407, тел. учёного секретаря: 209-52-04; e-mail: kochyn@bsu.by.

С диссертацией можно ознакомиться в Фундаментальной библиотеке Белорусского государственного университета.

Автореферат разослан « 21 » января 2025 г.

Учёный секретарь совета  
по защите диссертаций



В.П.Кочин

## ВВЕДЕНИЕ

В диссертации исследуются пороговые  $k$ -значные функции в связи с их применением в системах защиты информации, и изучается проблема построения аналитического задания произвольной пороговой  $k$ -значной функции, известная также как проблема характеристики пороговой  $k$ -значной функции. Применение пороговых функций в системах защиты информации объясняется простотой их технической реализации, согласованностью с логикой выполнения важнейших операций при обработке дискретной информации, высоким быстродействием и применением в нейροкомпьютерах. С методологической точки зрения данное исследование представляет интерес также в связи с развитием нейрокомпьютеров как новой вычислительной среды<sup>1, 2, 3</sup>.

Пороговая функция базируется на вычислении скалярного произведения на множестве действительных чисел и сравнения полученного результата с фиксированным порогом. Вычисление скалярного произведения является базовой операцией всех вычислительных платформ, как традиционных, так и перспективных<sup>1, 2, 3, 4, 5</sup>. Встроенность этой операции во внутреннюю логику ЭВМ делает пороговую функцию исключительно удобным базовым элементом, который получил широкое распространение и в универсальных, и в специальных вычислительных средствах<sup>3, 6, 7</sup>.

Внимание к изучению возможных приложений пороговых функций в немалой степени было инициировано также обнаружением пороговой природы работы нейронов живых организмов. В опубликованной в 1943 году работе<sup>8</sup> У. Маккалока и У. Питтса, на основании экспериментальных данных была построена модель так называемого формального нейрона, которая описывала работу нейронов с помощью булевых пороговых функций. Тот факт, что именно пороговые операции были отобраны природой в качестве базиса для выполнения высших функций мозга, явился исходным пунктом для широкого развития одного из важнейших направлений современной прикладной бионики –

---

<sup>1</sup> Розенблатт, Ф. Принципы нейродинамики. Перцептроны и теория механизмов мозга / Ф. Розенблатт ; пер. с англ. / В. Я. Алтаева [и др.] ; под ред. С. М. Осовца, – Москва : Мир, 1965. – 480 с.

<sup>2</sup> Бутаков, Е. А. Методы синтеза релейных устройств из пороговых элементов / Е. А. Бутаков. – М. : Энергия, 1970. – 328 с.

<sup>3</sup> Миркес, Е. М. Функциональные модели универсального нейрокомпьютера: дисс. ... д-ра техн. наук: 05.13.11 / Е. М. Миркес. – Красноярск, 2001. – 418 л.

<sup>4</sup> Дертоузос М. Пороговая логика / М. Дертоузос. – Москва: Мир, 1967. – 342 с.

<sup>5</sup> Widrow, B. Adaptive Switching Circuits / B. Widrow, M. E. Hoff. // IRE WESTCON Convention Record. – 1960. – Part 4. – P. 96–104.

<sup>6</sup> Минский, М. Перцептроны // М. Минский, С. Паперт – Москва: Мир, 1971. – 261 с.

<sup>7</sup> Hopfield, J. J. Neural networks and physical systems with emergent collective computational abilities / J. J. Hopfield // Proc. Natl. Acad. Sci. USA. – 1982. – Vol. 79, Issue 8. – P. 2554–2558.

<sup>8</sup> McCulloch, W.S. A logical calculus of the ideas immanent in nervous activity / W.S. McCulloch, W. Pitts // A Bulletin of Mathematical Biophysics. – 1943. – Vol. 5. – P. 115–133.

построению так называемых нейрокомпьютеров<sup>1, 8, 9, 10</sup>. Несмотря на обилие исследований в этой области, необходимо констатировать, что проблеме анализа реализуемых в нейрокомпьютере преобразований и защите данных в нейросетях уделяется мало внимания. Возникающие при этом задачи объективно сводятся к распознаванию пороговых элементов, их характеристике, причем не только в булевом, но и в  $k$ -значном случаях. Необходимость перехода в  $k$ -значную логику определилась благодаря обнаруженной уточненной природе нейронов, логика работы которых отвечает не булевым, а пороговым  $k$ -значным функциям<sup>9</sup>. Изучение пороговых  $k$ -значных функций и построенных на их основе сетей сделало заявленную проблему диссертации – характеристику пороговых  $k$ -значных функций – актуальной и практически значимой в своей прямой постановке.

Переход к переработке и передаче информации на новых физических принципах с высоким быстродействием стал ещё одним источником повышенного интереса к изучению базиса пороговых  $k$ -значных функций. В частности, использование оптических каналов связи и оптической вычислительной среды делает<sup>11, 12</sup> базис, состоящий из пороговых функций, самым удобным и согласованным с логикой переработки такой информации. Обращение к оптическим методам переработки и передачи информации, таким образом, также делает рассматриваемую в диссертации проблему характеристики пороговой  $k$ -значной функции актуальной и практически значимой.

Вместе с тем необходимо отметить, что в булевом случае данная задача известна достаточно давно<sup>1, 4</sup> и её решению были посвящены работы многих авторов<sup>1, 2, 4, 13, 14</sup>. Несмотря на известную простоту её постановки, задача проверки принадлежности конкретной функции классу пороговых функций и нахождения её аналитического задания оказалась достаточно сложной. В случае если функция действительно оказывалась пороговой, для нахождения её порогового представления предполагалась определенная итеративная

---

<sup>9</sup> Вальцев, В. Б. Некоторые структурные принципы организации высших функций мозга / В. Б. Вальцев, В. Р. Григорьев, В. Г. Никонов // «Нейрокомпьютер как основа мыслящих ЭВМ». – М.: Наука. – 1993. – с. 38–46.

<sup>10</sup> Терехин, А. Т. Нейросетевое моделирование когнитивных функций мозга: обзор основных идей / А. Т. Терехин, Е. В. Будилова, Л. М. Качалова, М.П. Карпенко // Психологические исследования: электрон. журн. – 2009. – N 2(4). – Режим доступа: <https://psystudy.ru/index.php/num/article/view/997/532> – Дата доступа: 2024.05.23.

<sup>11</sup> Белов П. А., Беспалов В. Н. и др. Оптические процессоры: достижения и новые идеи // Проблемы когерентной и нелинейной оптики. – СПб., 2006.

<sup>12</sup> Jahns J., Lee S. H. Optical Computing Hardware: Optical Computing // Elsevier Science, 1993.

<sup>13</sup> Chow, C. On the characterization of threshold functions. / C. Chow // In Proceedings of the Symposium on Switching Circuit Theory and Logical Design (FOCS). – 1961. – P. 34–38.

<sup>14</sup> Беляков-Бодин В. И., Розенблит С. И. Исследование некоторых вопросов синтеза пороговых функций // - М. Институт теоретической и экспериментальной физики Гос. Комитета по использованию атомной энергии СССР, 1972.

процедура. Разумеется, переход в  $k$ -значную ( $k > 2$ ) логику сопряжен с усложнением и развитием этих подходов.

Задача характеристики пороговых булевых и  $k$ -значных функций, сводящаяся<sup>15</sup> к решению систем линейных неравенств, приобрела<sup>16</sup> полиномиальную сложность благодаря результату Л. Хачияна. Высокая трудоемкость каждой итерации алгоритма эллипсоидов и их большое число оставили актуальной проблему поиска алгоритмов, менее трудоемких, чем алгоритм Хачияна. Отмеченная актуальность проблемы характеристики пороговых  $k$ -значных функций привлекла других авторов. Наиболее известной здесь оказалась работа З. Обрадовича<sup>17</sup>.

Теоретическая значимость данной диссертации заключается в построении нового алгоритма характеристики и доказательстве его сходимости за конечное число шагов. Ещё одним важным результатом диссертации стал тот факт, что построенный в ней геометрический алгоритм по всем параметрам улучшает алгоритм Обрадовича. Это стало возможным благодаря включению в геометрический алгоритм начальных параметров, в известном смысле обобщающих параметры Чоу<sup>13</sup> на случай  $k$ -значной логики, и оригинального геометрического метода их корректировки.

Актуальность темы диссертации определяется проходящим в настоящее время переходом на высокоскоростную передачу информации по современным и перспективным каналам связи, в частности оптическим, требующим разработки соответствующих систем защиты информации высокого быстродействия.

Проблема характеристики пороговых функций известна давно, с 60-х годов прошлого века, но она изучалась лишь для булевых функций. С наибольшей полнотой эта проблема рассматривалась в работах<sup>1, 2, 4, 14</sup>, для её решения, использовались параметры Чоу для первого приближения коэффициентов искомой линейной формы. Первые публикации по характеристике пороговых  $k$ -значных функций появились в 2000-х годах<sup>16, 18, 19</sup>. Это работы таких авторов как З. Обрадович, А. Нгом, М. Энтони, результаты которых служат отправной точкой для диссертационного исследования.

---

<sup>16</sup> Хачиян Л. Г. Полиномиальные алгоритмы в линейном программировании // ЖВМиМФ, 1980, вып. 20, №1, с. 51–68.

<sup>17</sup> Obradovic Z. Learning with Discrete Multi-Valued Neurons // Machine Learning: Proc. 7th Int'l. Conf., 1990, ed. B. W. Porter and R.J. Mooney, Austin, TX, Morgan-Kaufmann, pp. 392–399.

<sup>18</sup> Ngom A. Synthesis of Multiple-Valued Logic Functions by Neural Networks // Ph.D. Thesis Dissertation, Computer Science Department, University of Ottawa, Ontario, October 1998.

<sup>19</sup> Anthony M. Learning Multivalued Multithreshold Functions // CDAM Research Report LSE-CDAM-2003-03, January 2003.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

### **Связь работы с научными программами (проектами), темами**

Тема диссертации соответствует направлениям научных исследований, определенным Перечнем приоритетных направлений научных исследований Республики Беларусь «Методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантово-криптографические системы» (2011–2015 годы), «Безопасность человека, общества и государства» (2016–2020 годы) и «Средства технической и криптографической защиты информации, криптология и кибербезопасность» (2021–2025 годы).

### **Цель и задачи, объект и предмет исследования**

Цель диссертации – анализ комбинаторных свойств пороговых  $k$ -значных функций, разработка и анализ алгоритмов характеристики пороговой  $k$ -значной функции, позволяющих оценивать её параметры по столбцу значений.

Для достижения поставленной цели требуется решить следующие основные задачи:

1. Построение функционалов близости и отличия функций  $k$ -значной логики, аппроксимирующих коэффициенты линейной формы, для характеристики пороговой  $k$ -значной функции, и доказательство их свойств.

2. Разработка нового геометрического алгоритма характеристики пороговой  $k$ -значной функции на основе построенных функционалов и доказательство его сходимости за конечное число шагов.

3. Экспериментальное исследование свойств геометрического алгоритма характеристики, сравнение его характеристик с характеристиками алгоритма Обрадовича и алгоритма на основе метода эллипсоидов Хачияна; и разработка модификации геометрического алгоритма.

4. Применение разработанного геометрического алгоритма для решения задач анализа и синтеза узлов усложнения в системах защиты информации.

*Объектом исследования* являются пороговые  $k$ -значные функции, их способы задания, параметры и свойства. *Предметом исследования* являются методы характеристики пороговых  $k$ -значных функций.

### **Научная новизна**

Научная новизна диссертации заключается в принципиальной новизне разработанных в диссертации алгоритмов характеристики пороговых  $k$ -значных функций. Новыми являются и введенные характеристики: коэффициенты роста и возрастания, используемые для задания пороговой  $k$ -значной функции. Оригинальность построенного модифицированного геометрического алгоритма состоит в гибридном подходе к проблеме характеристики пороговых  $k$ -значных

функций, позволяющем осуществить балансирование между числом итераций алгоритма и числом обращений к вычислению значений функции. Новым является метод восстановления пороговой  $k$ -значной функции в узле защиты информации по неполным данным с помощью разработанного алгоритма характеристики.

#### **Положения, выносимые на защиту**

1. Теоретически доказанные и экспериментально установленные свойства функционалов близости и отличия функций  $k$ -значной логики, аппроксимирующих коэффициенты линейной формы.

2. Новый геометрический алгоритм характеристики пороговой  $k$ -значной функции и его модификация, направленная на снижение числа обращений к вычислению значений искомой функции.

3. Доказательство сходимости разработанного геометрического алгоритма характеристики пороговой  $k$ -значной функции и его модификации за конечное число шагов.

4. Результаты сравнительного анализа характеристик геометрического алгоритма и его модификации с характеристиками алгоритма Обрадовича и алгоритма на основе метода эллипсоидов Хачияна, демонстрирующие превосходство разработанных алгоритмов. При  $k > 4$  построенные алгоритмы дают преимущество в числе итераций алгоритма более чем в  $10^3$  раз, и с увеличением  $k$  и  $n$  это преимущество возрастает.

5. Результаты компьютерного моделирования геометрического алгоритма и его применения для решения задач анализа и синтеза узлов усложнения в системах защиты информации.

#### **Личный вклад соискателя ученой степени**

Основные результаты диссертационной работы получены соискателем самостоятельно. Научному руководителю в совместных работах принадлежат выбор направления исследований, предметные постановки задач, обсуждение результатов. Результаты, полученные другими соавторами или с другими соавторами, не вошли в диссертацию.

#### **Апробация диссертации и информация об использовании ее результатов**

Результаты диссертации прошли апробацию на научном семинаре кафедры математического моделирования и анализа данных Белорусского государственного университета (г. Минск, 10 октября 2017 г.); на конференции WebConf2018 «Веб-программирование и интернет-технологии» (г. Минск, 14–18 мая 2018 г.); XXVIII научно-практической конференции «Комплексная защита информации» (г. Гомель, 23–25 мая 2023 г.). Разработанные методы характеристики пороговых  $k$ -значных функций и их применение в задачах

защиты информации внедрены в лекционный курс, читаемый автором на кафедре математического моделирования и анализа данных факультета прикладной математики и информатики Белорусского государственного университета, что подтверждено актом внедрения. Также результаты диссертационной работы использованы для разработки программно-аппаратного комплекса ООО «Линфо» (г. Москва, Российская Федерация) и в исследованиях по специальной тематике в/ч 03405 (г. Минск, Республика Беларусь).

### **Опубликованность результатов диссертации**

Основные результаты диссертационной работы опубликованы в 10 научных работах, из которых: 5 статей в научных изданиях в соответствии с п. 19 Положения о присуждении ученых степеней и присвоении ученых званий (общий объем 3,59 авторского листа), 3 статьи в других научных изданиях, 2 материалов конференций и тезисов докладов.

### **Структура и объем диссертации**

Диссертация состоит из перечня сокращений и обозначений, введения, общей характеристики работы, четырех глав, заключения, списка литературы и Приложений, содержащих таблицы экспериментальных результатов оценивания трудоемкости разработанных алгоритмов и акты внедрения результатов диссертационного исследования. Полный объем диссертации составляет 131 страницу, в том числе 13 рисунков занимают 5 страниц, 21 таблица на 11 страницах, четыре приложения занимают 9 страниц. Список использованных источников содержит 96 наименований, включая собственные публикации соискателя ученой степени (на 9 страницах).

## **ОСНОВНАЯ ЧАСТЬ**

**В главе 1** введены определения пороговых булевых и  $k$ -значных функций, рассмотрены их основные свойства и осуществлен исторический обзор развития вопроса изучения данных классов функций.

**В разделе 1.1** рассмотрены булевы пороговые функции и история их изучения. В числе прочего рассмотрены вопросы их однородности, монотонности, самодвойственности, наличия запретов и сложности взаимной перестройки пороговых булевых функций. Приведены оценки числа пороговых функций, размаха пороговой булевой функции. Изложены основные методы распознавания пороговости булевой функции, свойства коэффициентов Чоу. Выделены наиболее изученные классы пороговых булевых функций: мажоритарные, равновероятные и линейно-разделимые.

**Определение 1.1** Булева функция  $f(x_1, \dots, x_n)$ , для которой существует линейная форма  $L(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$ ,  $x_i \in \{0,1\}$  с вещественными коэффициентами и вещественный порог  $T$  такие, что

$$f(x_1, \dots, x_n) = \begin{cases} 1, \text{ если } \sum_{i=1}^n a_i x_i \geq T \\ 0, \text{ если } \sum_{i=1}^n a_i x_i < T \end{cases},$$

называется пороговой булевой функцией. Пороговая булева функция может быть записана в следующем компактном виде:  $f = [a_1, a_2, \dots, a_n; T]$ .

**В разделе 1.2** рассмотрены свойства пороговых функций  $k$ -значной ( $k > 2$ ) логики. Изложена история изучения пороговых функций многозначной логики, которые с некоторых позиций можно рассматривать как промежуточный этап перехода к изучению пороговых  $k$ -значных функций. Далее вводится определение пороговой  $k$ -значной функций – основного объекта диссертационного исследования. Рассмотрены известные свойства данного класса: монотонность, абсолютная монотонность, инвариантность к преобразованиям однотипности, канонический набор весов, функциональная полнота. Рассмотрены параметры Номуры пороговых  $k$ -значных функций, обобщающие понятие коэффициентов Чоу на  $k$ -значную область и изложены их основные свойства.

**Определение 1.2** Функция  $k$ -значной логики  $f(x_1, \dots, x_n)$ , для которой существует линейная форма  $L(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$ ,  $x_i \in \{0,1, \dots, k-1\}$  с вещественными коэффициентами и вещественный порог  $T$  такие, что

$$f(x_1, \dots, x_n) = \begin{cases} 1, \text{ если } \sum_{i=1}^n a_i x_i \geq T \\ 0, \text{ если } \sum_{i=1}^n a_i x_i < T \end{cases},$$

называется пороговой функцией многозначной логики.

**Определение 1.3** Функция  $k$ -значной логики  $f(x_1, \dots, x_n)$ , для которой существует линейная форма  $L(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$ ,  $x_i \in \mathbb{Z}_k$  с вещественными коэффициентами и набор вещественных порогов  $b_0 < b_1 < \dots < b_k$  такие, что для всех  $i \in \overline{0, k-1}$  выполняется условие

$$f(x_1, \dots, x_n) = \begin{cases} 0, \text{ если } b_0 \leq L(x_1, \dots, x_n) < b_1 \\ 1, \text{ если } b_1 \leq L(x_1, \dots, x_n) < b_2 \\ \dots \\ k-1, \text{ если } b_{k-1} \leq L(x_1, \dots, x_n) < b_k \end{cases}, \quad (1)$$

называется пороговой  $k$ -значной функцией. Не ограничивая общность определения, можем положить здесь и далее  $b_0 = -\infty$  и  $b_k = +\infty$ . Пороговая  $k$ -значная функция может быть записана в следующем компактном виде:  $f = [a_1, a_2, \dots, a_n; b_1, b_2, \dots, b_{k-1}]$ .

**Раздел 1.3** посвящен истории исследования проблемы характеристики пороговых функций. Для булевого случая ( $k = 2$ ) характеристика пороговой функции может быть осуществлена несколькими способами: методом решения системы линейных неравенств в действительной области алгоритмом Хачияна либо алгоритмами внутренней точки, методом «Коррекции ошибки» Ф.Розенблатта, итеративным алгоритмом характеристики на базе характеристического вектора, методом табулирования, алгоритмом «Отделения» Н.Литтлстоуна и целым классом квазиаддитивных алгоритмов (алгоритмов, представляющих собой сочетание аддитивного метода «Коррекции ошибки» Ф.Розенблатта и мультипликативного алгоритма «Отделения» Н.Литтлстоуна). Далее изложена история исследования проблемы характеристики пороговых  $k$ -значных функций. Подробно рассмотрены алгоритм Обрадовича и  $k$ -значный алгоритм отделения. Основное отличие этих двух алгоритмов в различном способе коррекции линейной формы и порогов: в алгоритме Обрадовича – аддитивный, в  $k$ -значном алгоритме отделения – мультипликативный.

**В главе 2** предложены и исследованы свойства различных функционалов близости и отличия пороговых  $k$ -значных функций: мультипликативные коэффициенты, разностные коэффициенты, квадратичные коэффициенты, коэффициенты роста и коэффициенты возрастания.

**В разделе 2.1** даны основные определения и рассмотрен способ применения данных коэффициентов для характеристики пороговых  $k$ -значных функций.

**Определение 2.1** Для функции  $k$ -значной логики  $f(x_1, \dots, x_n)$  мультипликативным коэффициентом переменной  $x_i$  называется величина

$$\xi_i = \sum_{(x_1, \dots, x_n) \in \mathbb{Z}_k^n} x_i \cdot f(x_1, \dots, x_n).$$

**Определение 2.2** Для функции  $k$ -значной логики  $f(x_1, \dots, x_n)$  разностным коэффициентом переменной  $x_i$  называется величина

$$\eta_i = \sum_{(x_1, \dots, x_n) \in \mathbb{Z}_k^n} |x_i - f(x_1, \dots, x_n)|;$$

квадратичным коэффициентом переменной  $x_i$  называется величина

$$\delta_i = \sum_{(x_1, \dots, x_n) \in \mathbb{Z}_k^n} (x_i - f(x_1, \dots, x_n))^2.$$

**Определение 2.3** Для функции  $k$ -значной логики  $f(x_1, \dots, x_n)$  коэффициентом роста по переменной  $x_i$  называется величина

$$\Delta_i = \sum_{(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in \mathbb{Z}_k^{n-1}} (f(x_1, \dots, x_{i-1}, k-1, x_{i+1}, \dots, x_n) - f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)).$$

**Определение 2.4** Для функции  $k$ -значной логики  $f(x_1, \dots, x_n)$  коэффициентом возрастания по переменной  $x_i$  называется величина

$$\lambda_i = \sum_{(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in \mathbb{Z}_k^{n-1}} \sum_{l=0}^{k-2} \sum_{\varepsilon=l+1}^{k-1} (f(x_1, \dots, x_{i-1}, \varepsilon, x_{i+1}, \dots, x_n) - f(x_1, \dots, x_{i-1}, l, x_{i+1}, \dots, x_n)).$$

**В разделе 2.2** излагаются и доказываются некоторые свойства коэффициентов роста и возрастания. Функциональная зависимость между коэффициентами роста и мультипликативными коэффициентами позволяет не только упростить алгоритм их вычисления, но и предложить новый аналог параметров Номуры и коэффициентов Чоу в  $k$ -значном случае – вектор параметров возрастания. Для данного вектора удалось показать наличие свойств, аналогичных свойствам параметров Номуры. Учитывая способность коэффициентов роста более эффективно в сравнении с мультипликативными коэффициентами осуществлять характеризацию пороговой  $k$ -значной функции, перспективным видится изучение вектора параметров возрастания, который отличается от параметров Номуры заменой в нем мультипликативных коэффициентов на коэффициенты роста. Основные преимущества параметров Номуры при этом сохраняются.

**Теорема 2.1** При  $k = 2$  для всех  $i = \overline{1, n}$  коэффициенты роста и возрастания совпадают:  $\lambda_i = \Delta_i$ .

**Теорема 2.2** При  $k = 3$  для всех  $i = \overline{1, n}$  коэффициенты роста и возрастания связаны соотношением  $\lambda_i = 2\Delta_i$ .

**Определение 2.5** В пространстве  $\mathbb{Z}^n$  ортантом называется множество векторов, у которых знаки одинаковых координат совпадают.

**Теорема 2.3** Пусть пороговая функция  $k$ -значной логики  $f(x_1, \dots, x_n)$ , задается линейной формой  $L(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$ . Обозначим вектор  $\vec{L} = (a_1, a_2, \dots, a_n)$ . Тогда вектор коэффициентов роста  $(\Delta_1, \Delta_2, \dots, \Delta_n)$  и вектор коэффициентов возрастания  $(\lambda_1, \lambda_2, \dots, \lambda_n)$  лежат в одном ортанте с вектором  $\vec{L}$ . Другими словами, знаки соответствующих координат у всех трех векторов совпадают.

**Теорема 2.4** Коэффициенты возрастания и мультипликативные коэффициенты связаны соотношением

$$\lambda_i = 2\xi_i - (k - 1) \cdot \|f\|,$$

где  $\|f\|$  – сумма значений функции  $f$  по всем переменным (вес функции).

**Определение 2.6** Для  $k$ -значной функции  $f(x_1, \dots, x_n)$  вектором параметров возрастания называется упорядоченный набор весов  $(\lambda_0, \lambda_1, \dots, \lambda_n, n_0, n_1, \dots, n_{k-1})$ , где  $\lambda_i$  – коэффициенты возрастания,  $i = \overline{1, n}$ ,  $n_j = |f^{-1}(j)|$  – вес  $j$ -го слоя значений функции,  $j = \overline{0, k-1}$ .

Далее будем обозначать  $f(x) \rightarrow (\lambda_0, \lambda_1, \dots, \lambda_n, n_0, n_1, \dots, n_k)$ .

**Теорема 2.5** Если две различные функции имеют одинаковые векторы параметров возрастания, то они обе непороговые. Если две функции имеют векторы параметров возрастания, которые отличаются друг от друга только перестановкой коэффициентов  $\lambda_0, \lambda_1, \dots, \lambda_n$  и одна из них пороговая, то вторая функция также является пороговой и может быть задана системой пороговых неравенств первой функции с соответствующей перестановкой переменных линейной формы.

Теорема 2.5 развивает теоремы Чоу<sup>13</sup> на случай  $k \geq 2$  на основе параметров  $(\lambda_0, \lambda_1, \dots, \lambda_n)$ .

Напомним, что при действии на переменные  $(x_1, \dots, x_n)$  преобразованием, включающим перестановку переменных  $\pi(x_1, \dots, x_n) = (x_{\pi(1)}, \dots, x_{\pi(n)})$ ,  $\pi \in \mathfrak{S}_n$  и замену знаков логики отдельных переменных с помощью преобразования отрицания Лукашевича  $\chi_i(x_1, \dots, x_n) = (x_1, \dots, x_{i-1}, k-1-x_i, x_{i+1}, \dots, x_n)$ ,  $i = \overline{1, n}$  свойство принадлежности функции классу пороговых сохраняется.

**Теорема 2.6** Пусть  $f(x_1, \dots, x_n)$  –  $k$ -значная пороговая функция с вектором параметров возрастания  $f(x) \rightarrow (\lambda_0, \lambda_1, \dots, \lambda_n, n_0, n_1, \dots, n_k)$ , тогда верны следующие соответствия

$$f(\pi(x)) \rightarrow (\pi(\lambda_0, \lambda_1, \dots, \lambda_n), n_0, n_1, \dots, n_{k-1}),$$

$$f(\chi_i(x)) \rightarrow (\lambda_0, \dots, \lambda_{i-1}, 2(k-1) \sum_{x \in \mathbb{Z}_k^n} f(x) - \lambda_i, \lambda_{i+1}, \dots, c_n, n_0, n_1, \dots, n_{k-1}),$$

где  $i = \overline{1, n}$ .

**В разделе 2.3** проводится анализ коэффициентов роста и коэффициентов возрастания как модели первого приближения при характеристике  $k$ -значной пороговой функции, представляющего собой итерационный процесс приближения к решению. Экспериментально исследовано значение максимального угла между векторами коэффициентов роста и коэффициентов возрастания. Методом Монте-Карло получены экспериментальные значения доли функции, для которых векторы коэффициентов роста и коэффициентов возрастания дают разделяющую плоскость. Полученные результаты не позволяют сделать вывод об однозначном преимуществе одного из этих векторов.

**В главе 3** излагается основной результат диссертации – новый геометрический алгоритм характеристики пороговых  $k$ -значных функций и его модификация на основе введенных в главе 2 функционалов близости и отличия функций  $k$ -значной логики; доказывается сходимости, приводятся экспериментальные значения параметров их применения.

**В разделе 3.1** вводится определение «чистого разделения» областей значений пороговой  $k$ -значной функции линейной формой. В формализованном виде излагается геометрический алгоритм пороговых  $k$ -значных функций. Основная идея алгоритма состоит в использовании коэффициентов роста либо коэффициентов возрастания в качестве первичной аппроксимации линейной формы пороговой  $k$ -значной функции. Далее, в случае, когда полученная линейная форма не дает чистого разделения областей значений пороговой  $k$ -значной функции, осуществляется процедура корректировки линейной формы по двум выбранным точкам, в которых происходит нарушение такого разделения.

**Замечание 3.1** В силу неоднозначности задания пороговой функции будем полагать возможным использование порогов, удовлетворяющих нестрогому неравенству

$$b_0 \leq b_1 \leq \dots \leq b_k.$$

В случае равенства порогов  $b_i = b_{i+1}$  для некоторого  $i \in \overline{0, k-1}$ , очевидно функция  $f(x_1, \dots, x_n)$  не принимает значения  $i$ . Также далее будем полагать строгое двухстороннее неравенство в (1):

$$f(x_1, \dots, x_n) = i \Leftrightarrow b_i < L(x_1, \dots, x_n) < b_{i+1}.$$

Этого всегда можно добиться небольшим изменением соответствующего порога или весов.

**Определение 3.1** Условимся говорить, что линейная форма  $L(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$  дает «чистое разделение» областей значений пороговой  $k$ -значной функции  $f(x_1, \dots, x_n)$ , принимающей все значения из множества  $\mathbb{Z}_k$ , если для любого  $\alpha = \overline{0, k-2}$  выполняется строгое неравенство

$$\max_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\} < \min_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha+1} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\}.$$

Если это выполняется, то границы  $b_0, b_1, \dots, b_k$  можно определить, например, следующим способом:

$$b_\alpha = \min_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\}, \alpha = \overline{0, k-1},$$

$$b_k = \max_{f(\varepsilon_1, \dots, \varepsilon_n) = k-1} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\} + 1.$$

В случае, когда функция  $f(x_1, \dots, x_n)$  не принимает некоторых значений из множества  $\overline{0, k-1}$ , необходимо следующим образом убрать из рассмотрения соответствующие области значений: пусть функция  $f(x_1, \dots, x_n)$  принимает значения  $0 \leq \alpha_0 < \alpha_1 < \dots < \alpha_t < k$ ,  $0 < t < k$ . Тогда для всех  $i = \overline{0, t-1}$  необходимо проверить выполнение строгого неравенства

$$\max_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha_i} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\} < \min_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha_{i+1}} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\}.$$

Пороги в этом случае можно определить, например, по такому правилу: для всех значений  $\alpha_0, \dots, \alpha_t$  присвоить значения

$$b_{\alpha_i} = \min_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha_i} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\};$$

далее, если функция принимает значение  $k-1$ , то положить

$$b_k = \max_{f(\varepsilon_1, \dots, \varepsilon_n) = k-1} \{a_1 \varepsilon_1 + \dots + a_n \varepsilon_n\} + 1,$$

в противном случае положить  $b_k = +\infty$ ; для оставшихся значений  $j \in \mathbb{Z}_k \setminus \{\alpha_0, \dots, \alpha_t\}$  (которые не являются значениями функции  $f(x_1, \dots, x_n)$ ) начиная со старшего присвоить соответствующему порогу значение  $b_j = b_{j+1}$ .

Обозначим далее для всех  $i = \overline{0, k-1}$

$$\begin{aligned} F_i &= \{(x_1, \dots, x_n) \in \mathbb{Z}_k^n \mid f(x_1, \dots, x_n) = i\}, \\ \max(F_i) &= \max_{(x_1, \dots, x_n) \in F_i} \{L(x_1, \dots, x_n)\}, \\ x_{\max}(F_i) &= \{(x_1, \dots, x_n) \in \mathbb{Z}_k^n \mid L(x_1, \dots, x_n) = \max(F_i)\}, \\ \min(F_i) &= \min_{(x_1, \dots, x_n) \in F_i} \{L(x_1, \dots, x_n)\}, \\ x_{\min}(F_i) &= \{(x_1, \dots, x_n) \in \mathbb{Z}_k^n \mid L(x_1, \dots, x_n) = \min(F_i)\}. \end{aligned}$$

В случае если  $F_i = \emptyset$ , положим  $\max(F_i) = +\infty$ ,  $\min(F_i) = -\infty$ ,  $x_{\max}(F_i) = (-1, \dots, -1)$  и  $x_{\min}(F_i) = (-1, \dots, -1)$ .

**Геометрический алгоритм характеристики k-значных пороговых функций.**

Пусть пороговая функция  $f(x_1, \dots, x_n)$  принимает только значения  $0 \leq \alpha_0 < \alpha_1 < \dots < \alpha_t < k$ ,  $0 < t < k$ .

*Шаг 1. Инициализация.*

Проинициализировать вектор коэффициентов линейной формы коэффициентами роста либо коэффициентами возрастания:

$$(a_1, \dots, a_n) = (\Delta_1, \Delta_2, \dots, \Delta_n) \text{ либо } (a_1, \dots, a_n) = (\lambda_1, \lambda_2, \dots, \lambda_n).$$

*Шаг 2. Вычисление проверочной таблицы.*

Для всех  $i = \overline{0, t}$ , вычислить  $\min(F_{\alpha_i})$ ,  $\max(F_{\alpha_i})$ .

*Шаг 3. Проверка чистого разделения областей значений функции.*

Для каждого  $i = \overline{0, t-1}$  проверить выполнение неравенства

$$\max(F_{\alpha_i}) \geq \min(F_{\alpha_{i+1}}).$$

В случае выполнения неравенства для некоторого  $i \in \{0, \dots, t-1\}$  перейти к функции «Коррекция» с параметрами  $(\alpha_i, \alpha_{i+1})$ . В противном случае перейти к функции «Вычисление порогов».

*Функция «Коррекция».*

Входным параметром блока является пара  $(\alpha_i, \alpha_{i+1})$ .

1.1. Выбор точек

Произвольным образом выбрать точки  $x \in x_{\max}(F_{\alpha_i})$  и  $y \in x_{\min}(F_{\alpha_{i+1}})$ .

1.2. Коррекция линейной формы

Для всех  $j \in \overline{1, n}$  присвоить  $a_j = a_j - x_j + y_j$ .

### 1.3. Возврат в основной цикл

Вернуться в пункт 2 основного алгоритма

*Функция «Вычисление порогов».*

Для всех значений  $\alpha_0, \dots, \alpha_t$  присвоить значения

$$b_{\alpha_i} = \min_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha_i} \{a_1 \varepsilon_1 + \dots + a_n \varepsilon_n\}.$$

Если функция принимает значение  $k - 1$ , то положить

$$b_k = \max_{f(\varepsilon_1, \dots, \varepsilon_n) = k-1} \{a_1 \varepsilon_1 + \dots + a_n \varepsilon_n\} + 1,$$

в противном случае положить  $b_k = +\infty$ ; для оставшихся значений  $j \in \mathbb{Z}_k \setminus \{\alpha_0, \dots, \alpha_t\}$  (которые не являются значениями функции  $f(x_1, \dots, x_n)$ ) начиная со старшего присвоить соответствующему порогу значение  $b_j = b_{j+1}$ .

*Выход алгоритма:* векторы  $(a_1, \dots, a_n), (b_0, \dots, b_k)$ .

**В разделе 3.2** доказывается теорема о том, что геометрический алгоритм характеристики сходится за конечное число шагов и дает реализацию пороговой  $k$ -значной функции.

**Теорема 3.1** Если  $f(x_1, \dots, x_n)$  –  $k$ -значная пороговая функция, то геометрический алгоритм характеристики сходится за конечное число шагов и дает ее реализацию в виде  $f = [a_1, a_2, \dots, a_n; b_1, b_2, \dots, b_{k-1}]$ .

**В разделе 3.3** осуществлено экспериментальное исследование параметров вычислительной сложности геометрического алгоритма и его сравнение с алгоритмом Обрадовича. На основании полученных методом Монте-Карло экспериментальных данных сделан вывод о том, что геометрический алгоритм демонстрирует преимущество по сравнению с алгоритмом Обрадовича. В таблице 1 приведены значения трудоемкости – среднего арифметического числа итераций (для  $10^5$  смоделированных пороговых функций) для геометрического алгоритма на базе коэффициентов роста ( $MI_{n,k}^{Geom}(KR)$ ) и для алгоритма Обрадовича ( $MI_{n,k}^{Obr}$ ) для указанных значений  $(k, n)$ .

Таблица 1 – Экспериментальное сравнение трудоемкости алгоритмов

| (k, n)                | (2, 3) | (2, 5) | (2, 8) | (2, 12) | (3, 7) | (4, 5) | (5, 4) | (6, 3) | (12, 2) |
|-----------------------|--------|--------|--------|---------|--------|--------|--------|--------|---------|
| $MI_{n,k}^{Geom}(KR)$ | 0      | 0,22   | 1,29   | 17,3    | 14,3   | 14,7   | 17,6   | 7,96   | 6,03    |
| $MI_{n,k}^{Obr}$      | 10     | 49     | 731    | 59077   | 154814 | 181127 | 233198 | 91904  | 1068527 |

Из таблицы видно, что преимущество построенных алгоритмов тем выше, чем больше  $k$  и  $n$ . При  $k > 4$  построенные алгоритмы дают преимущество более чем в 1000 раз.

**В разделе 3.4** представлен модифицированный геометрический алгоритм характеристики пороговой  $k$ -значной функции, применение которого в среднем позволяет снизить количество обращений к вычислению значений искомой функции за счет увеличения числа итераций. Основная идея модификации заключается в переходе к коррекции линейной формы сразу после первого обнаружения нарушения «чистого разделения» областей значений пороговой  $k$ -значной функции полученной линейной формой. Доказывается сходимость модифицированного геометрического алгоритма. Экспериментальные исследования методом Монте-Карло показывают подавляющее преимущество как модифицированного, так и исходного геометрического алгоритма над алгоритмом Обрадовича по числу обращений к вычислению значений искомой пороговой  $k$ -значной функции. Наличие такой модификации позволяет при практическом применении алгоритма характеристики пороговых  $k$ -значных функций осуществлять «маневрирование» (компромисс) между общим количеством итераций и трудоёмкостью отдельной итерации в зависимости от конкретных характеристик среды реализации алгоритма и условий доступа к значениям искомой пороговой  $k$ -значной функции.

#### **Модификация геометрического алгоритма.**

##### *Шаг 1. Инициализация*

Проинициализировать вектор коэффициентов линейной формы коэффициентами роста либо коэффициентами возрастания:

$$(a_1, \dots, a_n) = (\Delta_1, \Delta_2, \dots, \Delta_n) \text{ либо } (a_1, \dots, a_n) = (\lambda_1, \lambda_2, \dots, \lambda_n).$$

Для всех  $i = 0, k-1$  присвоить  $\min(F_i) = +\infty$ ,  $\max(F_i) = -\infty$ .

##### *Шаг 2. Вычисление корректирующего преобразования*

Для каждого  $x = (x_1, \dots, x_n) \in \mathbb{Z}_k^n$  вычислить  $L(x_1, \dots, x_n)$  и сравнить со значением  $\min(F_{f(x)})$  и  $\max(F_{f(x)})$ .

Если  $L(x_1, \dots, x_n) < \min(F_{f(x)})$ , то

1. присвоить  $\min(F_{f(x)}) := L(x_1, \dots, x_n)$ ,  $x_{\min}(F_i) := x$ ;
2. присвоить  $j := f(x) - 1$  и пока  $\max(F_i) = -\infty$  и  $j > 0$  уменьшать значение:  $j--$ ;
3. если  $j > 0$ , то сравнить  $\min(F_{f(x)})$  и  $\max(F_j)$ : если  $\min(F_{f(x)}) \leq \max(F_j)$ , то перейти к функции «Коррекция» с параметрами  $(x_{\max}(F_j), x_{\min}(F_{f(x)}))$ .

Если  $L(x_1, \dots, x_n) > \max(F_{f(x)})$ , то

1. присвоить  $\max(F_{f(x)}) := L(x_1, \dots, x_n)$ ,  $x_{\max}(F_i) := x$ ;
2. присвоить  $j := f(x) + 1$  и пока  $\min(F_i) = +\infty$  и  $j > 0$  увеличивать значение  $j++$ ;
3. если  $j < k$ , то сравнить  $\max(F_{f(x)})$  и  $\min(F_j)$ :

если  $\max(F_{f(x)}) \geq \min(F_j)$ , то перейти к функции «Коррекция» с параметрами  $(x_{\max}(F_{f(x)}), x_{\min}(F_j))$ .

*Шаг 3. Вычисление порогов и выход алгоритма*

Если на 2 шаге для всех  $x \in \mathbb{Z}_k^n$  алгоритм ни разу не перешел к функции «Коррекция» и перешёл на шаг 3, то это означает, что текущая линейная форма дает чистое разделение областей значений функции.

Для всех значений  $\alpha_0, \dots, \alpha_t$ , из множества значений функции  $f$ , присвоить значения

$$b_{\alpha_i} = \min_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha_i} \{a_1 \varepsilon_1 + \dots + a_n \varepsilon_n\}.$$

Если функция принимает значение  $k - 1$ , то положить

$$b_k = \max_{f(\varepsilon_1, \dots, \varepsilon_n) = k-1} \{a_1 \varepsilon_1 + \dots + a_n \varepsilon_n\} + 1,$$

в противном случае положить  $b_k = +\infty$ ; для оставшихся значений  $j \in \mathbb{Z}_k \setminus \{\alpha_0, \dots, \alpha_t\}$  (которые не являются значениями функции  $f(x_1, \dots, x_n)$ ) начиная со старшего присвоить соответствующему порогу значение  $b_j = b_{j+1}$ .

*Функция «Коррекция».*

Входным параметром блока является пара векторов  $(u, v) \in \mathbb{Z}_k^{2n}$ .

1. Для всех  $j \in \overline{1, n}$  присвоить  $a_j = a_j - u_j + v_j$ .
2. Вернуться на шаг 1 основного цикла программы.

*Выход алгоритма:* векторы  $(a_1, \dots, a_n), (b_0, \dots, b_k)$ .

**Теорема 3.2** Модифицированный геометрический алгоритм характеристики произвольной пороговой  $k$ -значной функции сходится за конечное число шагов и дает ее реализацию.

**Теорема 3.3** Результаты работы геометрического алгоритма и модифицированного геометрического алгоритма всегда целочисленны.

**В разделе 4.1** построены и исследованы модели узлов защиты информации, использующие пороговые  $k$ -значные функций, проведены экспериментальные исследования свойств их выходных последовательностей. Доказан критерий равновесности пороговых булевых функций специального вида.

**Теорема 4.1.** Пороговая функция вида

$$f = \begin{cases} 1, & a_1(x_1 - \frac{1}{2}) + \dots + a_n(x_n - \frac{1}{2}) > 0 \\ 0, & a_1(x_1 - \frac{1}{2}) + \dots + a_n(x_n - \frac{1}{2}) \leq 0 \end{cases}, a_i \in \{-1, 0, 1\}, i \in \overline{1, n},$$

является равновесной тогда и только тогда, когда для любого  $(x_1, \dots, x_n) \in V_2^n$

$$a_1(x_1 - \frac{1}{2}) + \dots + a_n(x_n - \frac{1}{2}) \neq 0.$$

**Теорема 4.2.** Пороговая функция вида

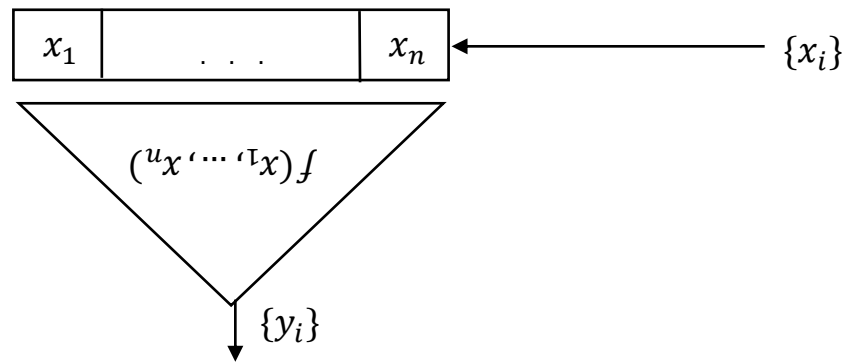
$$f = \begin{cases} 1, & a_1(x_1 - \frac{1}{2}) + \dots + a_n(x_n - \frac{1}{2}) > 0 \\ 0, & a_1(x_1 - \frac{1}{2}) + \dots + a_n(x_n - \frac{1}{2}) \leq 0 \end{cases}$$

$a_i \in \{-1, 0, 1\}$   $i \in \overline{1, n}$  является равновесной тогда и только тогда, когда число весовых коэффициентов  $a_i$ , не равных нулю, нечётно.

В разделе 4.2 рассмотрено применение разработанного геометрического алгоритма для анализа и синтеза узлов защиты информации на базе пороговых  $k$ -значных функций, доказана возможность успешной работы алгоритма при условии неполных данных

Рассмотрим узел, построенный на основе регистра сдвига и функции  $f(x_1, x_2, \dots, x_n)$  (рисунок 1), перерабатывающий входную последовательность  $\{x_i\}$  в выходную  $\{y_i\}$ . Рассматриваемый узел является важнейшим элементом усложнения в системах защиты информации и его анализу уделяется большое внимание.

Рассмотрим классическую задачу восстановления аналитического задания пороговой функции усложнения  $f(x_1, x_2, \dots, x_n)$  по известному входу и выходу.



**Рисунок 1 – Узел на основе регистра сдвига**

**Определение 4.1.** Функцию  $f(x_1, \dots, x_n): M \rightarrow \mathbb{Z}_k$ , где  $M \subseteq \mathbb{Z}_k^n$ , для которой существует линейная форма  $L(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$ ,  $x_i \in \mathbb{Z}_k$  с вещественными коэффициентами и набор вещественных порогов  $b_0 < b_1 < \dots < b_k$  такие, что для всех  $i \in \overline{0, k-1}$  выполняется условие

$$f(x_1, \dots, x_n) = i \Leftrightarrow b_i \leq L(x_1, \dots, x_n) < b_{i+1},$$

будем называть частично известной пороговой  $k$ -значной функцией. Не ограничивая общность определения, можем положить здесь и далее  $b_0 = -\infty$  и  $b_k = +\infty$ .

Будем называть геометрический алгоритм для характеристики  $k$ -значной пороговой функции, обрабатывающий точки из множества  $\mathbb{Z}_k \setminus M$  указанным выше способом, геометрическим алгоритмом для характеристики частично известной  $k$ -значной пороговой функции.

**Теорема 4.3** Пусть частично известная пороговая функция  $k$ -значной логики  $f(x_1, \dots, x_n)$ , задается линейной формой  $L(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$ . Обозначим вектор  $\vec{L} = (a_1, a_2, \dots, a_n)$ . Тогда вектор коэффициентов роста  $(\Delta_1, \Delta_2, \dots, \Delta_n)$  и вектор коэффициентов возрастания  $(\lambda_1, \lambda_2, \dots, \lambda_n)$  лежат в одном ортанте с вектором  $\vec{L}$  либо некоторые их координаты равны нулю. Другими словами, знаки соответствующих координат у всех трех векторов совпадают с точностью до равенства нулю.

**Теорема 4.4** Если  $f(x_1, \dots, x_n)$  – частично известная  $k$ -значная пороговая функция, то геометрический алгоритм характеристики частично известной  $k$ -значной пороговой функции сходится за конечное число шагов и дает ее реализацию.

Пусть множество

$$ML = \{L(x_1, \dots, x_n)\}$$

состоит из всех линейных форм, дающих чистое разделение областей значений функции  $f(x_1, \dots, x_n)$ . Определим верхние грани областей значений функции  $f(x_1, \dots, x_n)$ :

$$M_{\max} = \{(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_k^n \mid \exists L(x_1, \dots, x_n) \in ML : L(\alpha_1, \dots, \alpha_n) = \max(F_i), i = \overline{0, k-1}\},$$

и нижние грани областей значений функции  $f(x_1, \dots, x_n)$ :

$$M_{\min} = \{(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_k^n \mid \exists L(x_1, \dots, x_n) \in ML : L(\alpha_1, \dots, \alpha_n) = \min(F_i), i = \overline{0, k-1}\}.$$

Тогда указанный выше алгоритм характеристики частично известной функции позволяет восстановить параметры  $k$ -значной пороговой функции.

**В Приложении** к диссертации помещены: таблицы экспериментальных результатов оценивания трудоемкости геометрического алгоритма на базе коэффициентов роста (Приложение А); таблицы экспериментальных результатов оценивания трудоемкости геометрического алгоритма на базе

коэффициентов возрастания (Приложение Б); акты внедрения результатов диссертационного исследования (Приложение В).

## **ЗАКЛЮЧЕНИЕ**

### **Основные научные результаты диссертации**

1. Построен новый геометрический алгоритм характеристики пороговых  $k$ -значных функций. Данный алгоритм является принципиально новым; он использует особенности геометрического строения пороговой функций [4-А; 6-А; 7-А; 9-А].

2. Теоретически доказана сходимость геометрического алгоритма характеристики, а также его модификации за конечное число шагов. Этот результат имеет принципиальное значение при решении задачи характеристики пороговых  $k$ -значных функций [4-А; 8-А; 9-А].

3. Введены новые функционалы близости функций  $k$ -значной логики, имеющие практическое значение при характеристике пороговых  $k$ -значных функций: коэффициенты роста и коэффициенты возрастания. Данные коэффициенты расширяют инструментарий анализа пороговых  $k$ -значных функций [3-А; 4-А; 6-А; 7-А; 9-А].

4. Для введенных мультипликативных коэффициентов, коэффициентов роста и коэффициентов возрастания доказаны теоретические утверждения, устанавливающие взаимосвязи коэффициентов между собой и раскрывающие их роль в классификации и характеристике пороговых  $k$ -значных функций [3-А].

5. Проведен сопоставительный анализ нового построенного в диссертации алгоритма характеристики с алгоритмом Обрадовича, в результате которого установлено, что геометрический алгоритм значительно превосходит его по параметрам трудоемкости. Показано, что логическая простота геометрического алгоритма, а также низкая вычислительная сложность одной его итерации в большинстве случаев дает ему преимущество в сравнении с методом эллипсоидов Хачияна [1-А; 2-А].

6. Рассмотрено применение геометрического алгоритма для распознавания параметров узла защиты информации, реализованного пороговой  $k$ -значной функцией. Доказана возможность применения геометрического алгоритма для характеристики пороговой функции в узле защиты информации при неполных данных [1-А; 5-А; 10-А].

### **Рекомендации по практическому использованию результатов**

Полученные в диссертации результаты направлены на использование в задачах анализа и синтеза систем криптографической защиты информации высокого быстродействия. Результаты диссертации могут быть использованы в практических задачах восстановления параметров узла защиты информации,

реализованного пороговой  $k$ -значной функцией, а также в задаче восстановления аналитического задания пороговой функции усложнения при неполных данных. Результаты диссертации использованы в практических задачах защиты информации и в учебном процессе.

## **СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ**

### **Статьи в научных изданиях в соответствии с п. 19 Положения о присуждении ученых степеней и присвоении ученых званий**

1-А. Бурделёв, А. В. Распознавание параметров узла защиты информации, реализованного пороговой  $k$ -значной функцией / А. В. Бурделёв, В. Г. Никонов, И. И. Лапиков // Труды СПИИРАН. – 2016. – Вып. 46. – С. 108–127.

2-А. Бурделёв, А. В. Сравнительный анализ геометрического алгоритма и модифицированного метода эллипсоидов в задаче распознавания параметров узла защиты информации, реализованного  $k$ -значной пороговой функцией / А. В. Бурделёв, И. И. Лапиков // Интернет-журнал «Науковедение». – 2017. – Т. 9, №6. С. загл. с экрана.

3-А. Бурделёв, А. В. О свойствах коэффициентов роста и коэффициентов возрастания / А. В. Бурделёв // Лесной вестник / Forestry bulletin. – 2017. – Т. 21, Вып. 6. – С. 101–108.

4-А. Бурделёв, А. В. О сходимости нового алгоритма характеристики  $k$ -значных пороговых функций / А. В. Бурделёв // Прикладная дискретная математика. – 2018. – №39. – С. 107–115.

5-А. Бурделёв, А. В. Восстановление аналитического задания пороговой  $k$ -значной функции в узле защиты информации при неполных данных. / А. В. Бурделёв // Журнал Белорусского государственного университета. Математика. Информатика. – 2023. – №3. – С. 63–71.

### **Статьи в других научных изданиях**

6-А. Бурделёв, А. В. О построении аналитического задания  $k$ -значной пороговой функции / А. В. Бурделёв, В. Г. Никонов // Computational nanotechnology – 2015. – Вып. 2. – С. 5–13.

7-А. Бурделёв, А. В. О новом алгоритме характеристики  $k$  значных пороговых функций / А. В. Бурделёв, В. Г. Никонов // Computational nanotechnology. – 2017. – Вып. 1. – С. 7–14.

8-А. Бурделёв, А. В. Модификация геометрического алгоритма характеристики пороговых  $k$ -значных функций / А. В. Бурделёв // Computational nanotechnology. – 2018. – Вып. 1. – С. 132–138.

### **Материалы конференций и тезисы докладов**

9-А. Бурделёв, А. В. Пороговые  $k$ -значные функции, их характеристика и применение в системах защиты информации / А. В. Бурделёв // Веб-программирование и интернет-технологии WebConf2018: тез. докл.

4-й Междунар. науч.-практ. конф., Минск, 14–18 мая 2018 г. / Белорус. гос. ун-т; редкол.: И. М. Галкин (отв. ред.) [и др.]. – Минск, 2018. – С. 150.

10-А. Бурделёв, А. В. Восстановление аналитического задания пороговой k-значной функции в узле защиты информации при неполных данных / А. В. Бурделёв // Комплексная защита информации: материалы XXVIII научно-практической конференции, Гомель, 23-25 мая 2023 г. / УГЗ МЧС Республики Беларусь. – Минск, 2023. – С. 212–216.

**Бурдзялёў Аляксандр Уладзіміравіч**

**Парогавыя  $k$ -знакавыя функцыі, іх характарызацыя і прымяненне ў сістэмах абароны інфармацыі**

**Ключавыя словы:** парогавая  $k$ -значная функцыя, каэфіцыенты росту, каэфіцыенты ўзрастання, геаметрычны алгарытм характарызацыі парогавай  $k$ -значнай функцыі, збежнасць алгарытму, вузел абароны інфармацыі, алгарытм Абрадавіча, параметры Намуры.

**Мэта працы:** аналіз камбінаторных уласцівасцяў парогавых  $k$ -значных функцый, распрацоўка і аналіз алгарытмаў характарызацыі парогавай  $k$ -значнай функцыі, якія дазваляюць ацэньваць яе параметры.

**Метады даследвання:** дыскрэтная матэматыка, тэорыя булевых функцый і функцый  $k$ -значнай логікі, матэматычны аналіз, аналітычная геаметрыя, тэорыя верагоднасцяў, абарона інфармацыі, тэорыя алгарытмаў з ужываннем матэматычнага мадэлявання і кампутарных эксперыментаў.

**Атрыманыя вынікі і іх навізна.** У выніку праведзеных у дысертацыі даследаванняў пабудаваны новы геаметрычны алгарытм характарызацыі парогавых  $k$ -значных функцый, які выкарыстоўвае асаблівасці геаметрычнай будовы, а таксама ўведзены каэфіцыенты росту і ўзрастання. Тэарэтычна даказана збежнасць гэтага алгарытму за канчатковы лік крокаў. Параўнальны аналіз новага пабудаванага алгарытму і яго мадыфікацыі з алгарытмам Абрадавіча і алгарытмам на аснове метаду эліпсоідаў Хачыяна паказвае перавагу геаметрычнага алгарытму па характарыстыках працаёмкасці.

**Рэкамендацыі па выкарыстанні.** Атрыманыя ў дысертацыі вынікі накіраваны на выкарыстанне ў задачах аналізу і сінтэзы сістэм крыптаграфічнай абароны інфармацыі высокай хуткадзейнасці. Вынікі дысертацыі могуць быць выкарыстаны ў практычных задачах аднаўлення параметраў вузла абароны інфармацыі, рэалізаванага парогавай  $k$ -значнай функцыяй, а таксама ў задачы аднаўлення аналітычнага задання парогавай функцыі ўскладнення пры няпоўных дадзеных. Вынікі дысертацыі скарыстаны ў практычных задачах абароны інфармацыі і ў навучальным працэсе.

**Галіна прымянення:** абарона інфармацыі, дыскрэтная матэматыка.

**Бурделёв Александр Владимирович**

**Пороговые  $k$ -значные функции, их характеристика и применение в системах защиты информации**

**Ключевые слова:** пороговая  $k$ -значная функция, коэффициенты роста, коэффициенты возрастания, геометрический алгоритм характеристики пороговой  $k$ -значной функции, сходимость алгоритма, узел защиты информации, алгоритм Обрадовича, параметры Номуры

**Цель работы:** анализ комбинаторных свойств пороговых  $k$ -значных функций, разработка и анализ алгоритмов характеристики пороговой  $k$ -значной функции, позволяющих оценивать её параметры.

**Методы исследования:** дискретная математика, теория булевых функций и функций  $k$ -значной логики, математический анализ, аналитическая геометрия, теории вероятностей, защита информации, теория алгоритмов с применением математического моделирования и компьютерных экспериментов.

**Полученные результаты и их новизна.** В результате проведенных в диссертации исследований построен новый геометрический алгоритм характеристики пороговых  $k$ -значных функций, использующий особенности геометрического строения, а также введены коэффициенты роста и возрастания. Теоретически доказана сходимость этого алгоритма за конечное число шагов. Сопоставительный анализ нового построенного алгоритма и его модификации с алгоритмом Обрадовича и алгоритма на основе метода эллипсоидов Хачияна показывает превосходство геометрического алгоритма по характеристикам трудоемкости.

**Рекомендации по использованию.** Полученные в диссертации результаты направлены на использование в задачах анализа и синтеза систем криптографической защиты информации высокого быстродействия. Результаты диссертации могут быть использованы в практических задачах восстановления параметров узла защиты информации, реализованного пороговой  $k$ -значной функцией, а также в задаче восстановления аналитического задания пороговой функции усложнения при неполных данных. Результаты диссертации использованы в практических задачах защиты информации и в учебном процессе.

**Область применения:** защита информации, дискретная математика.

## SUMMARY

**Burdeliov Alexander Vladimirovich**

### **Threshold k-valued functions, their characterization and application in information security systems**

**Key words:** threshold k-valued function, growth coefficients, increasing coefficients, geometric algorithm for characterizing the threshold k-valued function, convergence of the algorithm, information security node, Obradovic algorithm, Nomura parameters.

**Purpose of the work:** analysis of combinatorial properties of threshold k-valued functions, development and analysis of algorithms for characterizing a threshold k-valued function, allowing to estimate its parameters.

**Research methods:** discrete mathematics, theory of Boolean functions and k-valued logic functions, mathematical analysis, analytical geometry, probability theories, information security, theory of algorithms using mathematical modeling and computer experiments.

**Obtained results and their novelty.** As a result of the research carried out in the dissertation, a new geometric algorithm for characterizing threshold k-valued functions was constructed, using the features of the geometric structure, and growth and increase coefficients were introduced. The convergence of this algorithm in a finite number of steps has been theoretically proven. A comparative analysis of the new constructed algorithm and its modification with the Obradovic algorithm and the algorithm based on the Khachiyan ellipsoid method shows the superiority of the geometric algorithm in terms of labor intensity characteristics.

**Recommendations for use.** The results obtained in the dissertation are aimed at using high-performance cryptographic information protection systems in problems of analysis and synthesis. The results of the dissertation can be used in practical problems of restoring the parameters of an information security unit implemented by a threshold k-valued function, as well as in the problem of restoring the analytical task of a threshold complication function with incomplete data. The results of the dissertation are used in practical problems of information security and in the educational process.

**Area of application:** information security, discrete mathematics.



Подписано в печать 13.01.2025. Формат 60×84  $\frac{1}{16}$ . Бумага офсетная.  
Ризография. Усл. печ. л. 1,39. Уч.-изд. л. 1,5.  
Тираж 60 экз. Заказ 2.

Отпечатано с оригинала-макета заказчика  
в республиканском унитарном предприятии  
«Издательский центр Белорусского государственного университета».  
Свидетельство о государственной регистрации издателя, изготовителя,  
распространителя печатных изданий № 2/63 от 19.03.2014.  
Ул. Красноармейская, 6, 220030, Минск.