Интернет-журнал «Науковедение» ISSN 2223-5167 https://naukovedenie.ru/

Том 9, №6 (2017) https://naukovedenie.ru/vol9-6.php

URL статьи: https://naukovedenie.ru/PDF/53TVN617.pdf

Статья опубликована 15.12.2017

Ссылка для цитирования этой статьи:
Лапиков И.И., Бурделев А.В. Сравнительный анализ геометрического метода и модифицированного метода эллисоидов в задаче распознавания параметров k-значной пороговой функции // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №6 (2017) https://naukovedenie.ru/PDF/53TVN617.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 512.55

Лапиков Игорь Игоревич
НКО «Фонд содействия развитию безопасных информационных технологий», Россия, Москва[1]
Сотрудник лаборатории
E-mail: Lapikov.I.I@yandex.ru
РИНЦ: http://elibrary.ru/author_profile.asp?id=955099

Бурделев Александр Владимирович
Белорусский государственный университет, Республика Беларусь, Минск
Старший преподаватель
E-mail: aburd2011@mail.ru

Сравнительный анализ геометрического метода и модифицированного метода эллисоидов в задаче распознавания параметров k-значной пороговой функции

Аннотация. В данной статье проводится сравнительный анализ двух авторских подходов к распознаванию параметров пороговых k-значных функций, которые могут быть использованы для построения узлов обработки и защиты информации. Сравнение параметров разработанных геометрического алгоритма и алгоритма, основанного на модифицированном методе эллипсоидов, осуществляется на общем полигоне из более чем 2,25 млн случайных пороговых функций, для характеризации которых используются предлагаемые подходы. В ходе экспериментальных исследований выявляются сильные и слабые стороны каждого из способов решения задачи характеризации пороговой k-значной функции и ставится задача по синтезу комбинированного подхода, нивелирующего недостатки каждого из методов, разработанных авторами. На практическом примере демонстрируются преимущества комбинированного подхода по сравнению с существующими.

Ключевые слова: пороговая k-значная функция; пороговая логика; метод эллипсоидов; характеризация пороговой функции

1. Введение (авторы Лапиков И. И., Бурделев А. В.)

Рассматриваемая в данной статье задача характеризации пороговой функции является классической задачей теории булевых функций и дискретной математики в целом [1, 2]. Несмотря на кажущуюся простоту постановки эта задача оказалась даже в булевой области

[1] 127287, Москва, проезд Старый Петровско-Разумовский, 1/23, стр. 1

весьма сложной, все подходы к решению которой носят итеративный характер. В то же время широкое прикладное применение пороговых булевых функций в различных системах переработки информации, включая системы защиты, приводит к продолжению исследований и поиску новых алгоритмов характеризации [3, 7, 11, 21, 22].

С другой стороны, на современном этапе развития информационных технологий тенденция к постоянному увеличению объемов перерабатываемой информации делает актуальной задачу перехода от битовых к k-значным преобразованиям. Построение архитектуры ЭВМ на основе k-значных преобразований влечет необходимость построения узлов защиты информации, основанных на преобразованиях данного типа. Стоит отметить еще одно актуальное направление использования k-значных преобразований – построение нейрокомпьютеров. Основным элементом нейрокомпьютеров являются формальные нейроны, функционирование которых описывается k-значными пороговыми функциями [28]. Построение систем защиты информации непосредственно в нейробазисе и определение параметров таких систем является важной с практической точки зрения задачей в области информационной безопасности. В общем случаем задача распознавания параметров k-значной пороговой функции или задача ее характеризации выходит за рамки исключительно задачи информационной безопасности, а является актуальной в целом для дискретной математики и различных приложений.

Определение 1. Функция k-значной логики $f^k(x_1,\ldots,x_n)$, для которой существует линейная форма $L(x_1,\ldots,x_n)=a_1x_1+a_2x_2+\ldots+a_nx_n$ с вещественными коэффициентами и набор вещественных порогов $b_0,b_1,\ldots,b_k$ такие, что для всех $i\in\overline{0,k-1}$ выполняется условие $f^k(x_1,\ldots,x_n)=i\Leftrightarrow b_i\le L(x_1,\ldots,x_n)<b_{i+1}$, называется *пороговой k-значной функцией*.

Определение 2. Под *алгоритмом характеризации пороговой k-значной функции*, понимается процедура нахождения какого-либо семейства параллельных гиперплоскостей, разделяющих множества различных значений данной функции, то есть нахождение коэффициентов $a_1,a_1,\ldots,a_n$ линейной формы $L(x_1,\ldots,x_n)$ и множества порогов $b_0,b_1,\ldots,b_k$.

В целом ряде разделов дискретной математики возникает задача распознавания принадлежности функции к некоторому классу и восстановления (характеризации) неизвестной дискретной функции из заданного класса с помощью последовательных вопросов о ее строении, например, о ее значениях в точках. В частности, известна сводимость к проблеме характеризации пороговой функции целого класса задач математической логики, математической экономики, целочисленного линейного программирования, теории распознавания образов. Приведем краткий обзор основных результатов и публикаций в данной области.

В работах [4, 5] рассматривалась задача построения алгоритма характеризации монотонных булевых и многозначных функций. В работе [1] показана сводимость задачи характеризации пороговой функции к задаче решения систем линейных неравенств в действительной области. Возможность применения алгоритма Хачияна [24] для характеризации пороговой функции исследована в работе [21]. В работах [2, 6] разобран итеративный алгоритм характеризации пороговой функции, который в качестве начального вектора коэффициентов разделяющей плоскости использует характеристический вектор булевой пороговой функции. Несмотря на наличие в работе [2] доказательства сходимости итеративного алгоритма и существования необходимого для сходимости вектора приращения, в ней остается открытым вопрос о скорости сходимости алгоритма и правиле выбора вектора приращения, для которого лишь указывается диапазон значений. В работах [7, 8] построен итеративный алгоритм характеризации пороговой функции, однако в качестве начального вектора значений выбирается произвольный вектор (по умолчанию – нулевой). Данный

алгоритм был предложен Ф. Розенблаттом в работе [7] и получил название «Метод коррекции ошибки». Далее М. Минским и С. Папертом [8] предложено несколько доказательств классической теоремы «О сходимости персептрона», устанавливающей сходимость алгоритма при любом начальном векторе. В своей работе М. Минский и С. Паперт привели строгое математическое доказательство того, что персептрон не способен к обучению в большинстве интересных для практического применения случаев. В работе [12] предложен алгоритм характеризации пороговых функций многозначной логики, представляющих собой модификацию алгоритма обучения персептрона Ф. Розенблатта. В 1990 году в работе сербского математика З. Обрадовича, выполненной под руководством И. Парберри, в Университете штата Пенсильвания [13] разработаны два алгоритма характеризации пороговой k-значной функции. Данные алгоритмы представляют собой модификации аддитивного алгоритма Розенблатта и мультипликативного алгоритма Литтлстоуна. Дальнейшее развитие алгоритма Обрадовича связано с обобщением понятия пороговой функции. В работе А. Нгома [14] дано обобщение алгоритма Обрадовича на случай немонотонной многозначной пороговой функции k-значной логики. Основные усилия автора модификации направлены на вычисление частичного порядка значений функции в слоях и применении алгоритма Обрадовича. В 2001 году появилась работа группы авторов с участием Н. Литтлстоуна [16], в которой осуществлено объединение двух классов алгоритмов характеризации булевой пороговой функции: аддитивного алгоритма Розенблатта и мультипликативного алгоритма Литтлстоуна – в класс квазиаддитивных алгоритмов. В работах [9, 10] Н. Ю. Золотых предложены алгоритмы характеризации пороговых функций многозначной логики, основанные на последовательном обращении к оракулу (условные тесты), в которых выбор точки для нового обращения к оракулу, определяется ответами на предыдущие вопросы.

Настоящая работа является логическим продолжением развития авторами подходов к проблеме характеризации пороговой k-значной функции, изложенных в работах [20, 21, 25]. Основной целью статьи является сравнение геометрического подхода, основанного на коэффициентах роста и возрастания [25] и модифицированного метода эллипсоидов для решения проблемы характеризации, а также выделение основных достоинств и недостатков этих методов

2. Геометрический алгоритм характеризации пороговых k-значных функций (автор Бурделев А. В.)

Изложим кратко основные положения геометрического подхода основанного на идее М. Дертоузоса использовать некоторый легко вычисляемый вектор, соответствующий мере близости функции $f(x)$ к функциям x_i, $i=\overline{1,n}$, в качестве первичной аппроксимации коэффициентов линейной формы, которая была перенесена в k-значную область. Впервые перенос данного инструмента в k-значную область осуществлен в предыдущих работах авторов [20, 21]. Таких мер близости двух k-значных функций может быть предложено несколько.

Определение 3. Для функции k-значной логики $f(x_1,\ldots,x_n)$ *мультипликативным коэффициентом* переменной x_i называется величина

$$\xi_i = \sum_{(x_1,\ldots,x_n)\in Z_k^n} x_i \bullet f(x_1,\ldots,x_n); \quad (1)$$

разностным коэффициентом переменной x_i называется величина

$$\eta_i = \sum_{(x_1,\ldots,x_n)\in Z_k^n} \left| x_i - f(x_1,\ldots,x_n) \right|; \quad (2)$$

квадратичным коэффициентом переменной x_i называется величина

$$\delta_i = \sum_{(x_1,\ldots,x_n)\in Z_k^n} \left(x_i - f\left(x_1,\ldots,x_n\right)\right)^2. \qquad (3)$$

Все введенные выше коэффициенты характеризуют меру близости функций $f\left(x_1,\ldots,x_n\right)$ и x_i, однако, как показали дополнительные исследования, для задачи нахождения даже первичного приближения аналитического представления k-значной пороговой функции они не подходят.

В булевой области, как уже было отмечено, для построения модели первого приближения коэффициентов линейной формы использовались коэффициенты Чоу, которые также рассматривались в работах [17, 18, 19], или на ином языке – коэффициенты характеристического вектора, которые можно трактовать как число знакоперемен функции по каждой координате. Продолжая эту аналогию при переходе к функциям k-значной логики можно ввести в рассмотрение коэффициенты роста, которые по каждой переменной подсчитывали бы величину возрастания значений функции и суммировали бы эти величины по всем ребрам, соответствующим выделенной переменной.

Определение 4. Для функции k-значной логики $f\left(x_1,\ldots,x_n\right)$ *коэффициентом роста по переменной* x_i называется величина

$$\Delta_i = \sum_{(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)} \left(f\left(x_1,\ldots,x_{i-1},k-1,x_{i+1},\ldots,x_n\right) - f\left(x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_n\right)\right). \qquad (4)$$

Другим параметром, представляющим интерес для характеризации k-значной пороговой функции, и более тонко учитывающим её строение, является коэффициент возрастания.

Определение 5. Для функции k-значной логики $f\left(x_1,\ldots,x_n\right)$ *коэффициентом возрастания по переменной* x_i называется величина

$$\lambda_i = \sum_{(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)\in Z_k^{n-1}} \sum_{l=0}^{k-2} \sum_{\varepsilon=l+1}^{k-1} \left(f\left(x_1,\ldots,x_{i-1},\varepsilon,x_{i+1},\ldots,x_n\right) - f\left(x_1,\ldots,x_{i-1},l,x_{i+1},\ldots,x_n\right)\right). \qquad (5)$$

Эксперименты показывают, что коэффициенты роста и коэффициенты возрастания наиболее удачно исполняют роль первичной аппроксимации коэффициентов линейной формы.

Замечание 1. В данной статье далее будем полагать строгое двухстороннее неравенство в определении пороговой k-значной функции:

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

Этого всегда можно добиться небольшим изменением соответствующего порога или весов, так как для любой пороговой функции набор весов и порогов не является однозначным.

Далее сформулируем новый алгоритм характеризации пороговых k-значных функций, который назовем геометрическим [25]. Пользуясь обозначениями определения 5, положим далее для всех $i = \overline{0,k-1}$.

$$F_i = \{\left(x_1,\ldots,x_n\right) \in Z_k^n \mid f\left(x_1,\ldots,x_n\right) = i\},$$

$$max\left(F_i\right) = \max_{(x_1,\ldots,x_n)\in F_i} \left\{L\left(x_1,\ldots,x_n\right)\right\},$$

$$x_{max}\left(F_i\right) = \{\left(x_1,\ldots,x_n\right) \in Z_k^n \mid L\left(x_1,\ldots,x_n\right) = max\left(F_i\right)\},$$

$$min\left(F_i\right) = \min_{(x_1,\ldots,x_n)\in F_i} \left\{L\left(x_1,\ldots,x_n\right)\right\},$$

$$x_{min}(F_i) = \{(x_1,\ldots,x_n) \in \mathsf{Z}_k^n \mid L(x_1,\ldots,x_n) = min(F_i)\}.$$

В случае если $F_i = \varnothing$, положим $max(F_i) = +\infty$ и $min(F_i) = -\infty$. Приведем геометрический алгоритм характеризации k-значных пороговых функций в формализованном виде.

Геометрический алгоритм характеризации пороговых k-значных функций (автор Бурделев А. В.)

1. Инициализация.

Проинициализировать вектор коэффициентов линейной формы коэффициентами роста либо коэффициентами возрастания:

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

2. Вычисление проверочной таблицы.

Вычислить $min(F_i)$, $max(F_i)$, $x_{min}(F_i)$, $x_{max}(F_i)$ для всех $i = \overline{0,k-1}$.

3. $ind = k-2$.

4. Удаление пустых строк из таблицы со сдвигом строк вверх.

Для каждого $i = \overline{0,k-1}$ такого, что $F_i = \varnothing$, выполнить:

а) для всех $j = \overline{i,ind}$ присвоить $min(F_i) = min(F_{i+1})$,

$$max(F_i) = max(F_{i+1}),\ x_{min}(F_i) = x_{min}(F_{i+1}),\ x_{max}(F_i) = x_{max}(F_{i+1});$$

б) $ind = ind - 1$.

5. Проверка чистого разделения областей значений функции.

Для каждого $i = \overline{0,ind}$ проверить выполнение неравенства

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

В случае выполнения неравенства для некоторого $i \in \{0,\ldots,ind\}$ вызвать блок «Коррекция» с параметром i и перейти на шаг 2 алгоритма.

В противном случае вызвать блок «Вычисление порогов» и завершить выполнение алгоритма.

Блок «Коррекция». Входным параметром блока является i.

1. Выбор точек.

Произвольным образом выбрать точки $u \in x_{max}(F_i)$ и $v \in x_{min}(F_{i+1})$.

2. Коррекция линейной формы.

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

3. Возврат в основной цикл.

Блок «Вычисление порогов».

Положить пороги

$$b_i = \min_{f(\varepsilon_1,\ldots,\varepsilon_n)=i}\{a_1\varepsilon_1+\ldots+a_n\varepsilon_n\}$$, для всех $i=\overline{0,k-1}$;

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

В случае если для некоторого $i=\overline{1,k-1}$ $F_i=\varnothing$, присвоить соответствующему порогу b_i любое значение из интервала между значениями порогов соседних областей. Если $F_0=\varnothing$, то положить $b_0=-\infty$.

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

Таким образом, на выходе итеративного алгоритма, будут два вектора: вектор коэффициентов линейной формы $(a_1,\ldots,a_n)$ и вектор порогов $(b_0,\ldots,b_k)$.

Пример 1. Найдем с помощью предложенного алгоритма реализацию пороговой 5-значной функции $f:\mathsf{Z}_5^5\to\mathsf{Z}_5$, задающейся линейной формой

$$L(x_1,\ldots,x_5)=x_1-25x_2+14x_3-43x_4+43x_5$$

и порогами $b_1=-164,\ b_2=-69,\ b_3=53,\ b_4=110$ следующим образом:

$$\begin{gathered} f(x_1,\ldots,x_5)=0\Leftrightarrow L(x_1,\ldots,x_5)<-164,\\ f(x_1,\ldots,x_5)=1\Leftrightarrow -164\le L(x_1,\ldots,x_5)<-69,\\ f(x_1,\ldots,x_5)=2\Leftrightarrow -69\le L(x_1,\ldots,x_5)<53,\\ f(x_1,\ldots,x_5)=3\Leftrightarrow 53\le L(x_1,\ldots,x_5)<110,\\ f(x_1,\ldots,x_5)=4\Leftrightarrow 110\le L(x_1,\ldots,x_5). \end{gathered} \qquad (6)$$

Предположим, что представление (6) неизвестно и на основании лишь табличного задания функции поставим задачу проверки принадлежности функции к классу пороговых и её характеризации. Вычислим коэффициенты возрастания данной функции:

$$(\lambda_{x_1},\lambda_{x_2},\lambda_{x_3},\lambda_{x_4},\lambda_{x_5})=(116,\ -3132,1766,\ -5444,5444).$$

В нашем примере наглядно видна корреляция между коэффициентами линейной формы и коэффициентами возрастания. Однако пороговая 5-значная функция, реализующаяся пороговым неравенством с коэффициентами $(\lambda_{x_1},\lambda_{x_2},\lambda_{x_3},\lambda_{x_4},\lambda_{x_5})$, не разделяет точно области значений функции f. Требуется проведение корректировки.

Вычислим значения $max(F_i)$ и $min(F_i)$ для линейной формы (см. таблицу 1)

$$L^{(1)}(x_1,\ldots,x_5)=116x_1-3132x_2+1766x_3-5444x_4+5444x_5.$$

Чистого разделения не происходит так как

$$max(F_1)=-8764>-8804=min(F_2).$$

Таблица 1

Значения $max(F_i)$ и $min(F_i)$ для линейной формы $L^{(1)}(x_1,\ldots,x_5)$

i	$min(F_i)$	$max(F_i)$
0	-34304	-20830
1	-20744	-8764

i	$min(F_i)$	$max(F_i)$
2	-8804	6622
3	6708	13832
4	13948	29304

Автор Бурделев А. В.

Проведем корректирование линейной формы $L^{(1)}(x_1,\ldots,x_5)$ в соответствии с общей логикой изложенного алгоритма. Для этого возьмем точки $(2,4,2,0,0)\in x_{max}(F_1)$ и $(4,0,4,3,0)\in x_{min}(F_2)$. Новая линейная форма

$$L^{(2)}(x_1,\ldots,x_5)=116x_1-3132x_2+1766x_3-5444x_4+5444x_5-2x_1-$$

$$-4x_2-2x_3+4x_1+4x_3+3x_4=118x_1-3136x_2+1768x_3-5441x_4+5444x_5$$

также не разделяет области значений функции f. Вычислим значения $max(F_i)$ и $min(F_i)$ для линейной формы $L^{(2)}(x_1,\ldots,x_5)$ (см. таблицу 2).

Таблица 2

Значения $max(F_i)$ и $min(F_i)$ для линейной формы $L^{(2)}(x_1,\ldots,x_5)$

i	$min(F_i)$	$max(F_i)$
0	-34308	-20824
1	-20728	-8760
2	-8779	6626
3	6716	13835
4	13950	29320

Автор Бурделев А. В.

Чистого разделения вновь не происходит, так как

$$max(F_1)=-8760>-8779=min(F_2).$$

Проведем вторую итерацию корректирования линейной формы $L^{(2)}(x_1,\ldots,x_5)$. Для этого выберем точки $(2,4,2,4,4)\in x_{max}(F_1)$ и $(4,0,4,3,0)\in x_{min}(F_2)$. Новая линейная форма

$$L^{(3)}(x_1,\ldots,x_5)=120x_1-3140x_2+1770x_3-5442x_4+5440x_5$$

дает чистое разделение областей значений функции f (см. таблицу 3).

Таблица 3

Значения $max(F_i)$ и $min(F_i)$ для линейной формы $L^{(3)}(x_1,\ldots,x_5)$

i	$min(F_i)$	$max(F_i)$
0	-34328	-20836
1	-20728	-8780
2	-8768	6610
3	6714	13820
4	13938	29320

Автор Бурделев А. В.

Далее выберем пороги по значениям $max(F_i)$, $i=\overline{1,3}$, после чего устанавливаем, что функция f реализуется линейной формой

$$L^{(3)}(x_1,\ldots,x_5)=120x_1-3140x_2+1770x_3-5442x_4+5440x_5$$

и порогами $b_1=-20836,\ b_2=-8780,\ b_3=6610,\ b_4=13820$.

3. Алгоритм характеризации пороговых k-значных функций на основе модифицированного метода эллипсоидов (автор Лапиков И. И.)

Как показано в работах [1, 21, 23], задача характеризации пороговой функции может быть сведена к анализу и решению систем линейных неравенств вида (7)

$$a_{i1}x_1+\ldots+a_{\text{in}}x_n\le b_i, i=1,\ldots,m. \quad (7)$$

В общем случае с теоретической точки зрения задача нахождения порогового представления k-значной функции $f^k(x_1,\ldots,x_n)$ сводится к решению системы неравенств, вообще говоря, двухсторонних для каждого значения i вида:

$$b_i\le a_1x_1+a_2x_2+\ldots+a_nx_n<b_{i+1},$$

где: $x_1,x_2,\ldots,x_n$ – известные координаты векторов, на которых функция принимает соответствующие значения, а параметры $a_1, a_2,\ldots, a_n, b_0, b_1,\ldots, b_k$ – неизвестные.

Действительно, если функция $f^k(x_1,\ldots,x_n)$ задана таблично и является пороговой, то ее значение в каждой точке $(x_1,\ldots,x_n)=(\varepsilon_1,\ldots,\varepsilon_n)$ приводит к формированию одного, вообще говоря, двустороннего неравенства вида:

$$f^k(x_1,\ldots,x_n)=i \Leftrightarrow b_i\le a_1\varepsilon_1+a_2\varepsilon_2+\ldots+a_n\varepsilon_n<b_{i+1}, \quad (8)$$

где: $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n$ – известные, принимают значения $\varepsilon_i\in\{0,\ldots,k-1\}$, а коэффициенты $a_1, a_2,\ldots, a_n$ и пороги $b_0, b_1,\ldots, b_k$ – неизвестны. Совокупность неравенств (8) для всех точек $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n)$ формирует систему

$$\begin{cases} b_0\le a_1\varepsilon_1^{(1)}+a_2\varepsilon_2^{(1)}+\ldots+a_n\varepsilon_n^{(1)}<b_1,\\ b_{k-1}\le a_1\varepsilon_1^{(k^n)}+a_2\varepsilon_2^{(k^n)}+\ldots+a_n\varepsilon_n^{(k^n)}<b_k. \end{cases}, \quad (9)$$

с целочисленными коэффициентами и действительными неизвестными. Полученная система (9) в точности соответствует системе линейных неравенств, рассмотренных Хачияном [24].

Сводимость задачи характеризации пороговой k-значной функции к системе линейных неравенств (9), показывает, что она имеет полиномиальную сложность благодаря возможности применения для ее решения полиномиального алгоритма Хачияна.

В [24] Л. Г. Хачиян показал возможность использования метода эллипсоидов для решения систем из $m\ge 2$ линейных неравенств относительно $n\ge 2$ действительных неизвестных $x_1, x_2, ..., x_n$:

$$\begin{cases} a_{11}x_1+\ldots+a_{1n}x_n\le b_1,\\ \ldots\\ a_{m1}x_1+\ldots+a_{mn}x_n\le b_m. \end{cases} \quad (10)$$

с целыми коэффициентами a_{ij}, b_i, для которой вводится понятие входа системы

$$L=\left[\sum\nolimits_{i,j=1}^{m,n}\log_2(|a_{i,j}|+1)+\sum\nolimits_{i=1}^{m}\log_2(|b_i|+1)+\log_2 mn\right]+1, \quad (11)$$

В лемме 1 работы [24] доказывается, что если система линейных неравенств (10) совместна, то она имеет решения в шаре радиуса 2^L, который в алгоритме Хачияна определяется, как начальная локализация области поиска решений. Далее в алгоритме строится последовательность эллипсоидов, описанных вокруг полушаров в n-мерном пространстве, которая центрами эллипсоидов осуществляет движение к области решений. Доказывается, что через $6n^2L$ итераций очередной центр эллипсоида либо оказывается решением системы (10), если система совместна, либо в случае несовместности системы (10), введенная автором невязка в центре эллипсоида будет больше определенного порогового значения.

Специфика решаемой в статье задачи потребовала введения в описанный алгоритм следующих модификаций, частично описанных в [26] и уточнения начальной локализации области решений. Исходя из разрядности современных процессоров было принято решение об ограничении области начальной локализации числами размеров в 16 байт, которое в свою очередь также является избыточным, поскольку разрядность современных процессоров составляет 8 байт. Наряду с критерием выхода по отрицательной невязке [26] алгоритма, введен критерий выхода по минимальному определителю. Напомним, что в ходе работы метода эллипсоидов строится последовательности эллипсоидов E_n задаваемых парой (x_n, B_n), где $x_n \in R$ – центр эллипсоида, а B_n – вещественная матрица. Поскольку матрица B_n выступает в качестве основной характеристики эллипсоида E_n, то предлагается использовать определитель матрицы B_n как один из критериев остановки. Эмпирическим путем установлено, что если $|detB_n| \le 10^{-9}$ и решение не было найдено, то необходимо остановить выполнение алгоритма, поскольку рассматриваемая система несовместна. Оценка скорости убывания модуля определителя позволяет существенно уменьшить максимальное количество итераций, которое в работе Л. Г. Хачияна получило оценку $6n^2L$, где n – количество неизвестных, а L – длина входа системы неравенств. Особенно эффективным данный критерий оказывается при использовании геометрического распараллеливания [27], поскольку в данном алгоритме используется методика доказательства несовместности в области разбиения, а начальные области поиска на каждом и потоков формируются в зависимости от задачи и аппаратных возможностей ЭВМ.

Дадим формальное описание алгоритма характеризации пороговой k-значной функции с использованием модифицированного метода эллипсоидов. Как уже было сказано, он состоит из двух этапов: этапа построения на основе табличного задания k-значной функции системы линейных неравенств вида (8) и непосредственно решения этой системы модифицированным методом эллипсоидов.

Алгоритм характеризации пороговых k-значных функций на основе модифицированного метода эллипсоидов (автор Лапиков И. И.)

1 Этап.

1.1. Построение табличного задания k-значной функции.

Инициализация векторов размерности n $\overline{\chi_p} = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n),\ \varepsilon_n m\left\{\overline{1, k-1}\right\},\ p\ m\left\{\overline{1, k^n}\right\}$.

1.2. Построение k-1 интервалов вида $(-\infty,\ b_0], [b_0, b_1), \ldots, [b_{k-2}, +\infty)$.

1.3. Формирование линейного неравенства для каждого вектора $\overline{\chi_p}$.

1.4. Формирование на основе неравенств из шага 1.3 матрицы $A=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$ коэффициентов СЛН и вектора свободных членов $b=\begin{pmatrix} b_1 \\ \dots \\ b_m \end{pmatrix}$.

2 Этап. Решение СЛН $A\bar{X} \le b$, *где* $\bar{X}$ *-вектор неизвестных.*

2.1. Инициализация начальных параметров метода эллипсоидов матрица коэффициентов A, вектора свободных членов b. начального радиуса шара области локализации решений $R = 2^{128}$, критериев выхода из алгоритма.

2.2. Инициализация шара (эллипсоида) начальной итерации параметрами x_0 и $B_0 = diag\,(R,\dots,R)$.

2.3. Вычисление невязки системы линейных неравенств и невязку алгоритма на k-ой итерации по формулам $\theta(T) = \max_{i=1\dots m}\left\{A_i T - b_i\right\}$ и $\theta_k = \min(\theta_{k-1}, \theta(x_{k-1}))$

2.4. Проверка выполнения критериев выхода.

2.5. Инициализация параметров нового эллипсоида

$\eta_k = B_k^T A_{i_k}^T$, где $i_k = \arg\max_{i=1\dots m}\left\{A_i\, x_k - b_i\right\}$, вектора

$$\overline{\eta_k} = \begin{pmatrix} \eta_1\eta_1 & \dots & \eta_1\eta_n \\ \dots & \dots & \dots \\ \eta_n\eta_1 & \dots & \eta_n\eta_n \end{pmatrix}.$$

Вычисление параметров нового эллипсоида

$$x_k \approx x_{k-1} - \frac{B_{k-1}\eta_{k-1}}{(n+1)\left\|\eta_{k-1}\right\|} \text{ и}$$

$$B_k \approx \left(1+\frac{1}{16n^2}\right)\frac{n}{\sqrt{(n^2-1)}}\left\{B_{k-1}\left[\sqrt{\left(\frac{n-1}{n+1}\right)}-1\right]\frac{B_{k-1}\eta_{k-1}}{\left\|\eta_k\right\|^2}\right\}.$$

Перейти к шагу 2.3.

Опишем основные критерии выхода из алгоритма.

1. Критерий выхода по отрицательной невязке системы линейных неравенств в центре эллипсоида $\theta(x_n)$.
2. Нулевое значение вектора η_k.
3. $\left|\det B_n\right| \le 10^{-9}$.

2.6. Выход из алгоритма: вектор решений $(x_1, x_2, \dots, x_n)$. В случае задачи характеризации последние k-1 элементов вектора следует трактовать как значение порогов. Если решение не найдено, то рассматриваемая функция не имеет порогового преставления.

Пример 2. Найдем с помощью модифицированного метода эллипсоидов реализацию пороговой 5-значной функции $f : \mathbb{Z}_5^5 \to \mathbb{Z}_5$ из примера 1, задающейся линейной формой

$$L(x_1,\ldots,x_5) = x_1 - 25x_2 + 14x_3 - 43x_4 + 43x_5$$

и порогами $b_1 = -164,\ b_2 = -69,\ b_3 = 53,\ b_4 = 110$ в соответствии с формулами (6).

Предположим, что представление (6) неизвестно и на основании лишь табличного задания функции поставим задачу проверки принадлежности функции к классу пороговых и её характеризации. На основании представления (6) и табличного задания функции f сформируем систему линейных неравенств. Эта система имеет вид (9) и состоит из 5747 линейных неравенств. Модифицированный методе эллипсоидов находит ее решение за 376 итераций с выходом по критерию отрицательной невязки в центре эллипсоида с вектором

$$\bar{X} = (a_1, a_2, a_3, a_4, a_5, b_0, b_1, b_2, b_3) = (2731, 59331272953; -66044, 17600557;$$

$$36691, 0069761194; -114154, 113263057; 113526, 457595585;$$
$$-438183, 3978049; -185828, 3821171; 136671, 8949790; 287147, 0708729)$$

Более высокая сложность по числу итераций модифицированного метода эллипсоидов в сравнении с геометрическим для данного примера, тем не менее, не дает оснований для общего вывода о преимуществе последнего. Во-первых, качество результатов сравнения зависит от вычислительной платформы, на которой реализованы оба алгоритма, а, во-вторых, существует множество примеров, для которых даже по числу итераций метод эллипсоидов выигрывает в сравнении с геометрическим методом. Один из таких примеров будет разобран ниже в заключительной части данной статьи.

Практические примеры применения алгоритма Хачияна и его модификаций выявили ещё одну особенность этого метода – рост модуля коэффициентов $a_j^{(i)}$ в ходе работы алгоритма. С целью получения дискретных значений текущие действительные выражения для $a_j^{(i)}$ требуют корректировки, для которой необходимо построение самостоятельной процедуры. Корректировка может включать процедуры деноминации текущих значений и их округления.

Определение 5. Под деноминацией будем понимать снижение значений a_i за счёт деления на 10^d при подходящим образом выбранном d. Коэффициент d будем называть порядком деноминации.

Проведем деноминацию значений полученного решения $\bar{X}$ с порядком 2

$$\bar{X} = (a_1, a_2, a_3, a_4, a_5, b_0, b_1, b_2, b_3) =$$
$$= (27; -660; 367; -1142; 1135; -4382; -1858; 1367; 2871)$$

В данном примере порядок деноминации f равен только 2, но практические эксперименты применения метода эллипсоидов для распознавания принадлежности произвольных k-значных функций показывают значительный рост порядка деноминации при увеличении количества аргументов функции. Это обусловливает необходимость проверки принадлежности полученного в результате деноминации и округления решения к многограннику решений рассматриваемой системы неравенств. Поскольку в примере найдено решение системы, принадлежащее многограннику её решений, можно сделать вывод, что функция f принадлежит к классу пороговых; если бы метод эллипсоидов показал несовместность системы, то можно было бы утверждать, что функция не является пороговой.

В работе [25] представлено сравнение геометрического алгоритма с алгоритмом Обрадовича. Приведем в таблице 4 сравнительные результаты параметров работы модифицированного метода эллипсоидов и геометрического метода.

Таблица 4

Результаты сравнения параметров работы модифицированного метода эллипсоидов и геометрического метода в задаче распознавания принадлежности произвольной функции к классу пороговых

n	k	Модифицированный метод эллипсоидов		Геометрический алгоритм.	
		$E_{\max}$	E_{med}	$G_{\max}$	G_{med}
2	2	6	3,625	1	1
2	3	25	11,85	1	1
2	4	51	25,07	4	1,15
2	5	82	47,28	6	1,17
2	21	1638	862,65	1109	147,29
3	2	12	6,28	1	1
3	3	46	24,8	7	1,23
3	4	108	59,5	14	1,58
3	5	172	109,4	41	2,7
3	19	2478	1586	42789	3496,87
4	2	23	10,71	2	1,05
4	3	94	52,14	15	1,6
4	4	211	127,41	5207	3,20
4	5	308	220,96	9355	12,04
4	10	1125	814	13525	956,55
5	2	34	17,81	3	1,23
5	3	155	98,46	44	2,95
5	4	309	230,47	637	14,68
5	5	528	382,8	2827	52,96
5	7	907	700,7	54273	559,5
6	2	63	29,7	9	1,48
6	3	286	174,88	257	7,24
6	4	481	385,1	2133	48,67
6	5	753	602,5	24356	222,17
7	2	114	50,98	18	1,7
7	3	409	294,16	569	18,28
7	4	722	574,69	9267	153,37
8	3	558	452,8	2038	48,66
8	3	558	452,8	2038	48,66
9	2	258	128,7	43	3,5
9	3	820	399,03	5822	116,7
15	2	1488	969,95	20482	99,27

Авторы Лапиков И. И., Бурделев А. В.

В таблице 4 использованы следующие обозначения: n – количество коэффициентов линейной формы, k – значность логики, $E_{\max}$ – максимальное количество итераций работы модифицированного метода эллипсоидов при заданных n и k, необходимых для решения задачи характеризации пороговой функции; E_{med} – среднее количество итераций работы модифицированного метода эллипсоидов при заданных n и k, необходимых для решения задачи характеризации пороговой функции; $G_{\max}$ – максимальное количество итераций работы геометрического алгоритма при заданных n и k, необходимых для решения задачи характеризации пороговой функции; G_{med} – среднее количество итераций работы

геометрического алгоритма при заданных n и k, необходимых для решения задачи характеризации пороговой функции.

Полученные статистические результаты обладают высокой степенью достоверности, поскольку сравнительный анализ проводился на большой выборке пороговых функций. В ходе эксперимента было сгенерировано более 2,25 млн пороговых функций с различными параметрами.

4. Заключение (автор Лапиков И. И.)

Проведенные эксперименты показывают, что каждый из рассмотренных алгоритмов обладает своей сферой предпочтительного применения. Значительно отличается характер роста сложности геометрического алгоритма и модифицированного метода эллипсоидов в зависимости от n и k, причем при увеличении k сложность геометрического алгоритма растет значительно быстрее, чем сложность метода эллипсоидов. К числу преимуществ метода эллипсоидов относится также его общая полиномиальная сложность с заведомо известной оценкой сложности как алгоритма в целом, так и одной итерации в частности.

В тоже время преимущества геометрического метода связаны с заведомо целочисленными значениями коэффициентов, доказанной сходимостью и возможностью для некоторых классов функций найти пороговое представление за одну итерацию.

Очевидным недостатком геометрического алгоритма является отсутствие общей оценки сложности, обнаруженная тенденция к росту модулей коэффициентов с увеличением числа итераций и отсутствие детерминированного доказательства непороговости функции.

Что же касается метода эллипсоидов то основным его недостатком можно считать высокую вычислительную сложность одной итерации и их общее количество, определяемое оценкой скорости убывания определителя матрицы, характеризующей эллипсоид.

Из всего изложенного вытекает естественное предложение построить комбинированный алгоритм, сочетающий положительные стороны каждого из двух рассмотренных. А именно способность геометрического алгоритма быстро найти приближение параметров пороговой функции можно использовать в методе эллипсоидов, рассматривая вектор, состоящий из этих параметров в качестве стартовой точки.

Практические эксперименты показывают, что использование первых приближений в качестве стартовой точки для метода эллипсоидов в случае, если функция имеет пороговое представление, значительно сокращает число итераций в методе эллипсоидов. В случае, если функция не имеет порогового представления, модифицированные метод эллипсоидов за известное число итераций покажет отсутствие такого представления.

Пример 3. Рассмотрим функцию f 4-значной функции $f : \mathrm{Z}_4^4 \to \mathrm{Z}_4$, задающуюся линейной формой

$$L(x_1,\ldots,x_5) = -2605x_1 - 2818x_2 + 2935x_3 - 4589x_4$$

и порогами $b_1 = 422,\ b_2 = 8243,\ b_3 = 12465$ следующим образом:

$$\begin{gathered} f(x_1,\ldots,x_5) = 0 \Leftrightarrow L(x_1,\ldots,x_5) < 422, \\ f(x_1,\ldots,x_5) = 1 \Leftrightarrow 422 \le L(x_1,\ldots,x_5) < 8243, \\ f(x_1,\ldots,x_5) = 2 \Leftrightarrow 8243 \le L(x_1,\ldots,x_5) < 12465, \\ f(x_1,\ldots,x_5) = 3 \Leftrightarrow 12465 \le L(x_1,\ldots,x_5). \end{gathered} \qquad (12)$$

Предположим, что представление (11) неизвестно и на основании лишь табличного задания функции поставим задачу проверки принадлежности функции к классу пороговых и её характеризации. Геометрический метод находит пороговое представление данной функции за 5207 итераций (при $G_{med} = 3,2$ для данных n и k). В результате работы алгоритма находится следующая линейная форма со с коэффициентами $a_1 = -97; a_2 = -105; a_3 = 112; a_4 = 174$ и порогами $b_1 = 22; b_2 = 319;\ \ b_3 = 482.$

Модифицированный метод эллипсоидов за 194 итерации определяет факт принадлежности данной функции к классу пороговых с вектором $X(-56090,5649;\ -60124,2277; 63662,603; 99580,01; 10677,4144;\ 180827,7466; 271315,9132)$. Используем комбинированный алгоритм для решения этой задачи. Для этого найдем первое приближение для коэффициентов линейной формы с использованием геометрического алгоритма. В результате работы на 4 итерации получим следующее приближение $(-57; -66;\ 67; 105)$. Построим для данной линейной формы приближение для значения порогов. Для это в линейную форму поставит значения $(0,0,0,0)$ $(1,1,1,1)$ $(2,2,2,2)$ $(3,3,3,3)$. Таким образом, получим стартовую точку для модифицированного метода эллипсоидов $\bar{X} = (a_1, a_2, a_3, a_4, b_0, b_1, b_2) = (-57; -66; 67; 105; 49; 98; 147)$. В результате работы алгоритма на 163 итерации получим вектор $X(-42849,9635; -46066,6081; 48083,4106; 75657,7071; 6643,1432;\ \ 136445,7472; 205840,4216)$. Проведем деноминацию и округление $X\ (-42850; -46067; 48083; 75657; 6643; 136445; 205840).$

Таким образом, можно сделать вывод, что использование в качестве первого приближения результатов работы геометрического алгоритма позволяет уменьшить количество итераций метода эллипсоидов, а метод эллипсоидов в данном примере на порядок быстрее геометрического метода находит пороговое представление функции. Стоит отметить, что еще одним неоспоримым достоинством комбинированного алгоритма является возможность классификации исследуемой функции как непороговой за счет доказательства несовместности СЛН, формируемых для метода эллипсоидов.

ЛИТЕРАТУРА

1. Бутаков, Е. А. Методы синтеза релейных устройств из пороговых элементов. М.: Энергия, 1970. 328 с.
2. Дертоузос М. Пороговая логика. М.: Мир, 1967. 342 с.
3. Зуев А. Ю. Пороговые функции и пороговые представления булевых функций // Математические вопросы кибернетики. 1994. № 5. С. 5-61.
4. 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.
5. 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.
6. В. И. Беляков-Бодин и С. И. Розенблит Исследование некоторых вопросов синтеза пороговых функций // Институт теоретической и экспериментальной физики Гос. Комитета по использованию атомной энергии СССР. 1972.
7. Розенблатт Ф. Принципы нейродинамики. Перцептроны и теория механизмов мозга. М.: Мир, 1963. 470 с.
8. Минский М., Паперт С. Персептроны. М: Мир, 1971. 263 с.
9. Золотых Н. Ю. Расшифровка пороговых и близких к ним функций многозначной логики: дисс. … канд. физ.-мат. наук: 05.13.17 / Золотых Николай Юрьевич. – Нижний Новгород, 1998. – 136 с.

10. Золотых Н. Ю. Расшифровка пороговых и близких к ним функций: дисс. ... доктора физико-математических наук: 01.01.09 / Золотых Николай Юрьевич; [Место защиты: Моск. гос. ун-т им. М. В. Ломоносова]. – Нижний Новгород, 2013. – 208 с.
11. Журавлев Ю. И. Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики. 1978. № 33. С. 5-68.
12. Nick Littlestone. Learning Quickly When Irrelevant Attributes Abound: A New Linear-Threshold Algorithm. Machine Learning. April 1988, Volume 2, Issue 4, pp. 285-318.
13. Obradovic, Z. and Parberry, I. "Learning with Discrete Multi-Valued Neurons," Machine Learning: Proc. 7th Int'l. Conf., ed. B. W. Porter and R. J. Mooney, Austin, TX, Morgan-Kaufmann, 1990. pp. 392-399.
14. Ngom A., Synthesis of Multiple-Valued Logic Functions by Neural Networks, Ph.D. Thesis Dissertation, Computer Science Department, University of Ottawa, Ontario, October 1998.
15. Anthony M. Learning Multivalued Multithreshold Functions. CDAM Research Report LSE-CDAM-2003-03, January 2003.
16. Grove A. J., Littlestone N., Schuurmans D. General Convergence Results for Linear Discriminant Updates. Machine Learning. 2001. № 43. pp. 173-210.
17. Chow C. On the characterization of threshold functions // Proceedings of the Symposium on Switching Circuit Theory and Logical Design (FOCS). 1961, pp. 34-38.
18. O'Donnell R., Servedio R. A. The Chow parameters problem // STOC. 2008. Pp. 517-526.
19. Anindya De, Diakonikolas Ilias. Nearly optimal solutions for the Chow Parameters Problem and low-weight approximation of halfspaces. Journal of the ACM (JACM). Volume 61 Issue 2, April 2014.
20. Бурделёв А. В., Никонов В. Г. О построении аналитического задания k-значной пороговой функции // Computational nanotechnology. 2015 Выпуск № 2. С. 5-13.
21. Бурделев А. В., Никонов В. Г., Лапиков И. И. Распознавание параметров узла защиты информации, реализованного пороговой k-значной функцией // Труды СПИИРАН. 2016. Вып. 46. С. 108-127.
22. Karmarkar N. «A New Polynomial Time Algorithm for Linear Programming», Combinatorica, 1984 Vol 4, nr. 4, pp. 373-395.
23. Филатов А. Ю. Развитие алгоритмов внутренних точек и их приложение к системам неравенств: дисс. ... кандидата физ.-мат. наук: 05.13.18. – Иркутск, 2001. – 123 с.
24. Хачиян Л. Г. Полиномиальные алгоритмы в линейном программировании // «Журнал вычислительной математики и математиче ской физики», 1980, Т 20.
25. А. В. Бурделёв, В. Г. Никонов, О новом алгоритме характеризации k-значных пороговых функций // Comp. nanotechnol., 2017. Вып. 1, С. 7-14.
26. Лапиков И. И., Никонов В. Г. Адаптивный алгоритм решения систем линейных неравенств с k-значными неизвестными // Труды Военно-космической академии им. А. Ф. Можайского, 2016, №650, С. 88-94.
27. Лапиков И. И. О возможности геометрического распараллеливания адаптивного алгоритма решения систем неравенств с k-значными неизвестными на базе метода эллипсоидов Хачияна // Системы управления и информационные технологии, 2016. №2. С. 14-19.
28. Вальцев В. Б., Григорьев В. Р., Никонов В. Г. Некоторые структурные принципы организации высших функций мозга // «Нейрокомпьютер как основа мыслящих ЭВМ. – М.: Наука, 1993. С. 38-46.

Lapikov Igor Igorevich
NPO «FSTRBIT», Russia, Moscow
E-mail: Lapikov.I.I@yandex.ru

Burdelev Alexander Vladimirovich
Belarus state university, Belarus, Minsk
E-mail: aburd2011@mail.ru

Comparative analysis of the geometric method and the modified ellipsoids method in the k-valued threshold function parameters recognition problem

Abstract. This article discusses a comparative analysis of two author's approaches to the recognition of the parameters of the threshold k-valued functions, which can be used for building information processing and security units. Comparison of parameters of the developed geometrical algorithm and the algorithm based on a modified ellipsoid's method is made on a common polygon of more than 2,25 million random threshold functions, for the characterization of which the proposed approaches are used. The pilot study identifies advantages and disadvantages of each method used for the characterization of threshold k-valued function. The aim of the study is a synthesis of a combined approach that mitigates the drawbacks of each method developed by the authors. A practical example demonstrates the advantages of the combined approach compared to existing ones.

Keywords: threshold k-valued function; threshold logic; ellipsoid method; the characterization of threshold functions