УДК 519.65

ВОССТАНОВЛЕНИЕ АНАЛИТИЧЕСКОГО ЗАДАНИЯ ПОРОГОВОЙ *k*-ЗНАЧНОЙ ФУНКЦИИ В УЗЛЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ НЕПОЛНЫХ ДАННЫХ

А. В. БУРДЕЛЁВ[1)]

[1)]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Рассматривается задача восстановления пороговой функции в узле защиты информации по входу и выходу в случае, когда известны не все значения. Для решения этой задачи предлагается использовать геометрический алгоритм характеризации частично известной пороговой *k*-значной функции. Доказывается сходимость алгоритма на конечном шаге, а также показывается, что в результате работы алгоритма будет построена некоторая пороговая функция, совпадающая с данной функцией во всех известных точках.

Ключевые слова: алгоритм характеризации; доказательство сходимости; пороговая функция; коэффициенты роста; коэффициенты возрастания.

Образец цитирования:
Бурделёв АВ. Восстановление аналитического задания пороговой *k*-значной функции в узле защиты информации при неполных данных. *Журнал Белорусского государственного университета. Математика. Информатика.* 2023;3:63–71.
EDN: XPGVEV

For citation:
Burdeliov AV. Restoration of the analytical task of the threshold *k*-valued function in the information protection node with incomplete data. *Journal of the Belarusian State University. Mathematics and Informatics.* 2023;3:63–71. Russian.
EDN: XPGVEV

Автор:
Александр Владимирович Бурделёв – преподаватель кафедры математического моделирования и анализа данных факультета прикладной математики и информатики.

Author:
Alexander V. Burdeliov, lecturer at the department of mathematical modelling and data analysis, faculty of applied mathematics and computer science.
aburd2011@mail.ru
https://orcid.org/0009-0009-1177-3635

CC BY NC

Журнал Белорусского государственного университета. Математика. Информатика. 2023;3:63–71
Journal of the Belarusian State University. Mathematics and Informatics. 2023;3:63–71

RESTORATION OF THE ANALYTICAL TASK OF THE THRESHOLD *k*-VALUED FUNCTION IN THE INFORMATION PROTECTION NODE WITH INCOMPLETE DATA

A. V. BURDELIOV [a]

[a]*Belarusian State University, 4 Niezaliezhnasci Avenue, Minsk 220030, Belarus*

This article considers the problem of restoring the threshold function in the information protection node from a input and output in the case when not all values are known. To solve this problem, it is proposed to use a geometric algorithm for characterising a partially known threshold *k*-valued function. The article proves the convergence of the algorithm at the final step; it is also shown that as a result of the algorithm, a certain threshold function will be constructed, which will coincide with this function at all known points.

Keywords: algorithm of learning of threshold functions; proof of convergence; threshold function; expansion coefficients; increase coefficients.

Введение

Рассмотрим задачу восстановления аналитического задания функции усложнения $f(x_1, \ldots, x_n)$ в узле защиты информации по известным входу и выходу. В случае применения пороговой *k*-значной функции в роли функции усложнения задача нахождения ее аналитического задания может быть успешно решена по входу и выходу с помощью геометрического алгоритма характеризации пороговых *k*-значных функций, введенного в работах [1; 2].

Пороговые функции и их характеризация

Определение 1 [3]. Функция *k*-значной логики $f(x_1, \ldots, x_n)$, для которой существуют линейная форма $L(x_1, \ldots, x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$, $x_i \in \mathbb{Z}_k$, с действительными коэффициентами и набор действительных порогов $b_1 < b_2 < \ldots < b_k$ такие, что для всех $i \in \overline{0,\ k-1}$ выполняется условие

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

называется пороговой *k*-значной функцией. Не ограничивая общности определения, можем положить, что здесь и далее $b_0 = -\infty$ и $b_k = +\infty$. Пороговую *k*-значную функцию будем писать в следующем сокращенном виде: $f = \left[a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_{k-1}\right]$.

Под алгоритмом характеризации пороговой *k*-значной функции понимается процедура нахождения какого-либо семейства параллельных гиперплоскостей, разделяющих множества различных значений данной функции, т. е. процедура нахождения коэффициентов $a_1, a_2, \ldots, a_n$ линейной формы $L(x_1, \ldots, x_n)$ и множества порогов $b_1, b_2, \ldots, b_{k+1}$. Отметим, что задача характеризации пороговой функции имеет не единственное решение (например, все коэффициенты линейной формы и пороги могут быть домножены на ненулевой коэффициент). Кроме того, каждой пороговой функции f можно поставить в соответствие класс $\mathfrak{L}_f$ векторов коэффициентов линейной формы и порогов, реализующих данную пороговую функцию:

$$\mathfrak{L}_f = \left\{ \left(a_1, a_2, \ldots, a_n, b_0, b_1, \ldots, b_{k+1}\right) \middle| f = \left[a_1, a_2, \ldots, a_n; b_0, b_1, \ldots, b_{k-1}\right] \right\}.$$

В целом ряде разделов дискретной математики возникает задача распознавания принадлежности функции некоторому классу и восстановления (характеризации) неизвестной дискретной функции из заданного класса с помощью последовательных вопросов о ее значениях в точках. Нахождение параметров пороговой булевой функции является объективно более сложной математической задачей, чем определение принадлежности функции классу пороговых функций, и сводится к итеративной процедуре.

Рассмотрение задачи нахождения параметров пороговой функции в *k*-значной логике ставит первый важный вопрос о возможных вариантах трактовки близости или отличия двух *k*-значных функций, а в случае решения задачи нахождения аналитического представления *k*-значных функций – вопрос о вариантах трактовки их близости к функциям x_i. Может быть предложено несколько мер близости двух *k*-значных функций.

Определение 2 [1; 2; 4]. Для функции *k*-значной логики $f(x_1, \ldots, x_n)$ коэффициентом роста по переменной x_i называется величина

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

Определение 3 [1; 2; 4]. Для функции k-значной логики $f(x_1, \ldots, x_n)$ коэффициентом возрастания по переменной x_i называется величина

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

Геометрический алгоритм характеризации пороговых *k*-значных функций

В работах [1; 2] вводится геометрический алгоритм характеризации пороговых k-значных функций, при этом в статье [2] доказывается его сходимость на конечном шаге.

Условие 1. В силу неоднозначности задания пороговой функции будем полагать возможным использование порогов, удовлетворяющих нестрогому неравенству $b_0 \le b_1 \le \ldots \le b_k$. В случае равенства порогов $b_i = b_{i+1}$ для некоторого $i \in \overline{0, k-1}$ очевидно, что функция $f(x_1, \ldots, x_n)$ не принимает значения i. Также далее будем полагать справедливым строгое двустороннее неравенство в определении пороговой k-значной функции:

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

Этого всегда можно добиться небольшим изменением соответствующего порога или весов.

Определение 4 [1; 2]. Будем говорить, что линейная форма $L(x_1, \ldots, x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$ дает чистое разделение областей значений пороговой k-значной функции $f(x_1, \ldots, x_n)$, принимающей все значения из множества $\mathbb{Z}_k$, если для любого $\alpha = \overline{0, k-2}$ выполняется строгое неравенство

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

Если оно выполняется, то пороги $b_0, b_1, \ldots, b_k$ можно определить, например, следующим способом:

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

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

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

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

При его выполнении пороги можно определить, например, по правилу: для всех значений $a_0, \ldots, a_t$ присвоить значения $b_{\alpha_i} = \min\limits_{f(\varepsilon_1, \ldots, \varepsilon_n) = \alpha_i} \{a_1\varepsilon_1 + \ldots + a_n\varepsilon_n\}$; если функция принимает значение $k-1$, положить, что $b_k = \max\limits_{f(\varepsilon_1, \ldots, \varepsilon_n) = k-1} \{a_1\varepsilon_1 + \ldots + a_n\varepsilon_n\} + 1$, в противном случае положить, что $b_k = +\infty$; для оставшихся значений $j \in \mathbb{Z}_k \backslash \{a_0, \ldots, a_t\}$ (которые не являются значениями функции $f(x_1, \ldots, x_n)$) присвоить соответствующему порогу, начиная со старшего, значение $b_j = b_{j+1}$.

Далее для всех $i = \overline{0, k-1}$ введем обозначения

$$F_i = \left\{(x_1, \ldots, x_n) \in \mathbb{Z}_k^n \,\middle|\, f(x_1, \ldots, x_n) = i\right\},$$

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

$$x_{\max}(F_i) = \left\{(x_1, \ldots, x_n) \in \mathbb{Z}_k^n \middle| L(x_1, \ldots, x_n) = \max(F_i)\right\},$$

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

$$x_{\min}(F_i) = \left\{(x_1, \ldots, x_n) \in \mathbb{Z}_k^n \middle| L(x_1, \ldots, x_n) = \min(F_i)\right\}.$$

Если $F_i = \varnothing$, положим, что $\max(F_i) = +\infty$, $\min(F_i) = -\infty$, $x_{\max}(F_i) = (-1, \ldots, -1)$ и $x_{\min}(F_i) = (-1, \ldots, -1)$.

Приведем геометрический алгоритм характеризации пороговых k-значных функций.

Вход алгоритма: вектор значений функции $f(x_1, \ldots, x_n)$.

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

Шаг 1: инициализация. Проинициализировать начальный вектор коэффициентов линейной формы коэффициентами роста либо коэффициентами возрастания:

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

Шаг 2: вычисление проверочной таблицы. Для всех $i = \overline{0, t}$ вычислить $\min\left(F_{\alpha_i}\right)$, $\max\left(F_{\alpha_i}\right)$.

Шаг 3: проверка чистого разделения областей значений функции. Для каждого $i = \overline{0, t-1}$ проверить выполнение неравенства

$$\max\left(F_{\alpha_i}\right) < \min\left(F_{\alpha_{i+1}}\right).$$

При выполнении неравенства для некоторого $i \in \{0, \ldots, t-1\}$ перейти к блоку коррекции с параметрами $\left(a_i, a_{i+1}\right)$. В противном случае перейти к блоку вычисления порогов.

Блок коррекции. Входным параметром блока является пара $\left(a_i, a_{i+1}\right)$.

Шаг 1: выбор точек. Произвольным образом выбрать точки $(x_1, \ldots, x_n) \in x_{\max}\left(F_{\alpha_i}\right)$ и $(y_1, \ldots, y_n) \in$ $\in x_{\min}\left(F_{\alpha_{i+1}}\right)$.

Шаг 2: коррекция линейной формы. Для всех $j \in \overline{1, n}$ присвоить $a_j = a_j - x_j + y_j$.

Шаг 3: возврат в основной цикл. Вернуться к шагу 2 основного цикла алгоритма.

Блок вычисления порогов. Для всех значений $a_0, \ldots, a_t$ присвоить значения

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

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

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

в противном случае положить, что $b_k = +\infty$; для оставшихся значений $j \in \mathbb{Z}_k \setminus \{a_0, \ldots, a_t\}$ (которые не являются значениями функции $f(x_1, \ldots, x_n)$) присвоить соответствующему порогу, начиная со старшего, значение $b_j = b_{j+1}$.

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

Восстановление аналитического задания пороговой *k*-значной функции в узле защиты информации при неполных данных

Как правило, при решении задачи восстановления аналитического задания функции усложнения $f(x_1, \ldots, x_n)$ в узле защиты информации по известным входу и выходу в распоряжении имеются значения функции $f(x_1, \ldots, x_n)$ не во всех точках. В этом случае на задачу характеризации пороговой функции накладываются дополнительные ограничения – неполные данные.

Определение 5. Функцию $f(x_1, \ldots, x_n): M \to \mathbb{Z}_k$, где $M \subseteq \mathbb{Z}_k^n$, для которой существуют линейная форма $L(x_1, \ldots, x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$, $x_i \in \mathbb{Z}_k$, с действительными коэффициентами и набор действительных порогов $b_0 < b_1 < \ldots < b_k$ такие, что для всех $i \in \overline{0, k-1}$ выполняется условие

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

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

Под алгоритмом характеризации частично известной пороговой k-значной функции понимается процедура нахождения какого-либо семейства параллельных гиперплоскостей, разделяющих множества различных значений данной функции, т. е. процедура нахождения коэффициентов $a_1, a_2, \ldots, a_n$ линейной формы $L(x_1, \ldots, x_n)$ и множества порогов $b_0, b_1, \ldots, b_{k+1}$.

Рассмотрим применение геометрического алгоритма для характеризации частично известной пороговой k-значной функции. Для этого следует определиться, как действовать геометрическому алгоритму, когда он обращается к точке, в которой значение искомой функции неизвестно, т. е. в терминах определения 5 обращается к точке из множества $\mathbb{Z}_k \backslash M$.

Геометрический алгоритм обращается к значениям функции в следующих случаях:

1) при подсчете коэффициентов роста либо коэффициентов возрастания для первичной аппроксимации линейной формы;

2) при вычислении максимумов и минимумов значений линейной формы в областях значений искомой функции.

Наиболее простым и логичным действием при отсутствии информации о значении функции в точке видится игнорирование данной точки, которое в обоих случаях должно быть реализовано следующим образом:

1) при подсчете коэффициентов роста

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

либо коэффициентов возрастания

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

в соответствующих им суммах игнорируются слагаемые, для вычисления которых осуществляется обращение к неизвестному значению искомой функции;

2) при вычислении максимума ($\max\left(F_{\alpha_i}\right)$) и минимума ($\min\left(F_{\alpha_i}\right)$) значений линейной формы в областях значений искомой функции следует игнорировать значение линейной формы в данной точке.

Определение 6. Геометрический алгоритм характеризации пороговой k-значной функции, обрабатывающий точки из множества $\mathbb{Z}_k \backslash M$ указанным выше способом, будем называть геометрическим алгоритмом характеризации частично известной пороговой k-значной функции.

Актуальным вопросом является сходимость данного алгоритма. Для доказательства сходимости необходимо рассмотреть вопрос принадлежности к одному ортанту вектора коэффициентов роста, вектора коэффициентов возрастания и вектора коэффициентов линейной формы частично известной пороговой k-значной функции.

Теорема 1. *Пусть частично известная пороговая k-значная функция* $f(x_1, \ldots, x_n)$ *задается линейной формой*

$$L(x_1, \ldots, x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n.$$

Введем вектор коэффициентов линейной формы $\vec{L}(a_1, a_2, \ldots, a_n)$. *Тогда вектор коэффициентов роста* $(\Delta_1, \Delta_2, \ldots, \Delta_n)$ *и вектор коэффициентов возрастания* $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ *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.*

Доказательство. Согласно работе [4] пороговая k-значная функция является полностью монотонной, т. е. для любого $s \le n$, любого подмножества переменных $x_{i_1}, \ldots, x_{i_s}$ и любых двух фиксаций переменных $\left(x_{i_1}, \ldots, x_{i_s}\right) = (\varepsilon_1, \ldots, \varepsilon_s)$, $\left(x_{i_1}, \ldots, x_{i_s}\right) = (\delta_1, \ldots, \delta_s)$ соответствующие этим фиксациям подфункции

$$f_\varepsilon = \Big(x_1, \ldots, x_n \Big| \left(x_{i_1}, \ldots, x_{i_s}\right) = (\varepsilon_1, \ldots, \varepsilon_s)\Big),$$

$$f_\delta = \Big(x_1, \ldots, x_n \Big| \left(x_{i_1}, \ldots, x_{i_s}\right) = (\delta_1, \ldots, \delta_s)\Big)$$

удовлетворяют одному из следующих условий: либо $f_\varepsilon \le f_\delta$, либо $f_\varepsilon \ge f_\delta$. Исключение из рассмотрения некоторых значений пороговой k-значной функции не нарушает ее полную монотонность. Таким образом, частично известная пороговая k-значная функция является полностью монотонной.

Рассмотрим фиксации переменной x_j значениями $x_j = p$ и $x_j = p + 1$ для некоторого $p = \overline{0,\ k-2}$. Для любого значения $p = \overline{0,\ k-2}$ соотношение между фиксациями f_p и f_{p+1} определяется только соответствующим знаком коэффициента линейной формы a_j: если $a_j > 0$, то $f_p \le f_{p+1}$; если $a_j = 0$, то $f_p = f_{p+1}$; если $a_j < 0$, то $f_p \ge f_{p+1}$.

Тогда слагаемые из определения 2

$$\xi_{KR} \equiv f\left(x_1, \ldots, x_{j-1}, k-1, x_{j+1}, \ldots, x_n\right) - f\left(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n\right)$$

и слагаемые из определения 3

$$\xi_{KV} \equiv \sum_{l=0}^{k-2} \sum_{\varepsilon=l+1}^{k-1} \left(f\left(x_1, \ldots, x_{j-1}, \varepsilon, x_{j+1}, \ldots, x_n\right) - f\left(x_1, \ldots, x_{j-1}, l, x_{j+1}, \ldots, x_n\right)\right)$$

имеют одинаковый знак с коэффициентом линейной формы a_j либо равны нулю. Суммы значений ξ_{KR} и ξ_{KV}, соответствующие значениям коэффициента роста Δ_i и коэффициента возрастания λ_i, имеют одинаковый знак (либо равны нулю), и этот знак совпадает со знаком коэффициента линейной формы a_j. В случае, когда $a_j = 0$, суммы значений ξ_{KR} и ξ_{KV} также будут равны нулю. Теорема 1 доказана.

Теорема 2. *Если $f\left(x_1, \ldots, x_n\right)$ – частично известная пороговая k-значная функция, то геометрический алгоритм характеризации частично известной пороговой k-значной функции сходится за конечное число шагов и дает ее реализацию.*

Доказательство. Пусть пороговая k-значная функция $f\left(x_1, \ldots, x_n\right)$ задается линейной формой $L\left(x_1, \ldots, x_n\right) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$. Введем вектор коэффициентов линейной формы $\vec{L}\left(a_1, a_2, \ldots, a_n\right)$. Вокруг вектора $\vec{L}$ всегда можно построить конус допустимых решений Q такой, что любой вектор, лежащий в данном конусе, будет давать чистое разделение областей значений функции $f\left(x_1, \ldots, x_n\right)$ [5]. Напомним, что для конуса выполняются два свойства:

- $\vec{\alpha} \in Q \Rightarrow k\vec{\alpha} \in Q$ для всех $k > 0$;
- $\vec{\alpha} \in Q,\ \vec{\beta} \in Q \Rightarrow \left(\vec{\alpha} + \vec{\beta}\right) \in Q$.

Конусом допустимых решений Q назовем такой конус, в котором для любого $\vec{\alpha} \in Q$ линейная форма, построенная по коэффициентам вектора $\vec{\alpha}$, дает чистое разделение областей значений функции $f\left(x_1, \ldots, x_n\right)$.

Угол раствора конуса обозначим через Θ ($\Theta > 0$).

Докажем, что за конечное число шагов алгоритма вектор коэффициентов линейной формы окажется внутри конуса допустимых решений.

По теореме 1 вектор коэффициентов роста и вектор коэффициентов возрастания лежат в одном ортанте с вектором $\vec{L}$. Таким образом, алгоритм начинает работу с вектора $\vec{A}_0$, лежащего в одном ортанте с вектором $\vec{L}$.

Рассмотрим операцию коррекции в алгоритме. Пусть $\vec{A}_i$ – текущий вектор линейной формы, который поступает на вход блока коррекции. После коррекции он переходит в вектор $\vec{A}_{i+1}$.

Алгоритм осуществляет коррекцию с помощью двух точек – $u_i \in x_{\max}\left(F_{a_j}\right)$ и $v_i \in x_{\min}\left(F_{a_{j+1}}\right)$ – тогда и только тогда, когда одновременно выполняются два неравенства:

- $\vec{A}_i v_i \le \vec{A}_i u_i$ (так как задействован блок коррекции алгоритма);
- $\vec{L} v_i > \vec{L} u_i$ (в силу определения 1).

Эти неравенства равносильны системе

$$\begin{cases} \vec{L}\left(v_i - u_i\right) > 0, \\ \vec{A}_i\left(v_i - u_i\right) \le 0. \end{cases} \tag{1}$$

Вектор коррекции $\left(v_i - u_i\right) \equiv \vec{C}_i$ прибавляется к текущему вектору $\vec{A}_i$ и получается новый вектор $\vec{A}_{i+1}$:

$$\vec{A}_{i+1} = \vec{A}_i + \vec{C}_i.$$

Рассмотрим плоскость, на которой лежат векторы $\vec{L}$ и $\vec{A}_i$ (рис. 1). Обозначим через $\vec{C}_{LA_i}$ проекцию вектора $\vec{C}_i$ на плоскость, образованную векторами $\vec{L}$ и $\vec{A}_i$. Перенесем начало этой проекции в конец вектора $\vec{A}_i$.

В силу первого неравенства системы (1) конец вектора $\vec{C}_{LA_i}$ должен быть ниже прямой q, в силу второго неравенства системы (1) конец вектора $\vec{C}_{LA_i}$ должен быть выше прямой p, т. е. лежать в заштрихованной области на рис. 1. Таким образом, вектор $\vec{C}_{LA_i}$ направлен к вектору $\vec{L}$.

Рассмотрим конус K_i, образованный вращением вектора $\vec{A}_i$ вокруг вектора $\vec{L}$. Очевидно, что вектор $\vec{C}_i$, приложенный к окончанию вектора $\vec{A}_i$, заходит внутрь конуса K_i. Для каждого шага алгоритма возможны два случая: вектор $\vec{C}_i$ целиком лежит внутри конуса K_i или вектор $\vec{C}_i$ выходит за пределы конуса K_i, т. е. «прокалывает» конус, как на рис. 2.

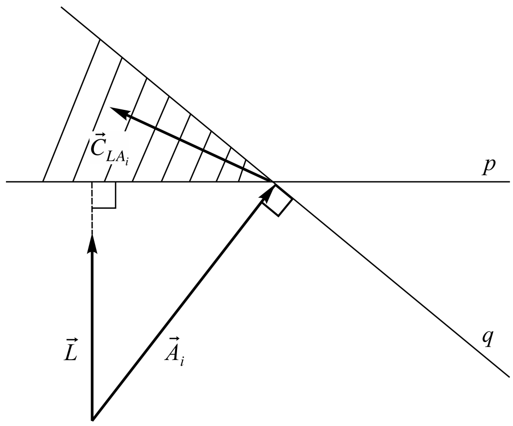

Рис. 1. Проекция вектора коррекции
Fig. 1. Projection of the correction vector

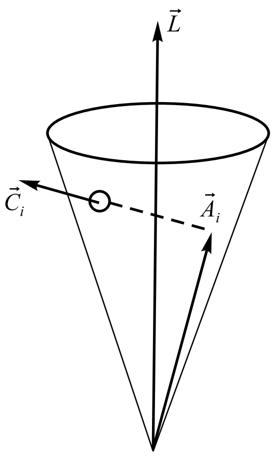

Рис. 2. «Прокол» конуса
Fig. 2. «Puncture» of the cone

Далее покажем, что «прокол» конуса может произойти конечное число раз. Так как по условию 1 для любых $u_i, v_i \in \mathbb{Z}_k^n$ выполняется неравенство

$$\vec{L}\left(v_i - u_i\right) > 0,$$

то существует δ > 0 такое, что для любых $u_i, v_i \in \mathbb{Z}_k^n$

$$\vec{L}\left(v_i - u_i\right) > r.$$

Это означает, что часть заштрихованной области на рис. 1, заведомо содержащая конец вектора $\vec{C}_{LA_i}$, лежит на $\dfrac{r}{|L|}$ выше (по нормали к плоскости p), чем окончание вектора $\vec{A}_i$. Рассмотрим рис. 3, являющийся модификацией рис. 1 с учетом вышеизложенного. Расстояние от конца проекции вектора $\vec{C}_i$ на плоскость основания конуса K_i до касательной к окружности конуса K_i в точке окончания вектора $\vec{A}_i$ будет не менее чем d.

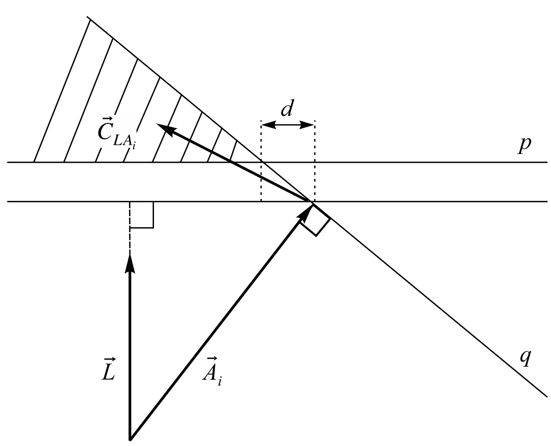

Рис. 3. Проекция вектора коррекции после модификации
Fig. 3. Projection of the correction vector after modification

Нижнюю границу для расстояния d определяет тот факт, что угол между векторами $\vec{A}_i$ и $\vec{L}$ составляет не менее чем Θ (иначе алгоритм останавливает работу) и менее чем $\frac{\pi}{2} - \Theta$. Таким образом,

$$d \geq \frac{r}{|L|} \operatorname{tg}\Theta > 0.$$

Длина вектора $\vec{C}_i$ ограничена сверху величиной $(k-1)\sqrt{n}$.

На рис. 4 изображены две окружности – окружность основания конуса K_i вокруг вектора $\vec{L}$ и окружность радиусом $(k-1)\sqrt{n}$ вокруг окончания вектора $\vec{A}_i$. К окружности основания конуса K_i проведена касательная в точке окончания вектора $\vec{A}_i$. На расстоянии d от касательной проведена линия.

Согласно вышеизложенному окончание проекции вектора $\vec{C}_i$ на плоскость основания конуса K_i должно лежать на расстоянии не менее чем d от касательной, на расстоянии не более чем $(k-1)\sqrt{n}$ от окончания вектора $\vec{A}_i$ и по одну сторону с вектором $\vec{L}$ относительно касательной. Таким образом, окончание проекции вектора $\vec{C}_i$ лежит в заштрихованной области (см. рис. 4).

Легко заметить, что заштрихованная область не целиком лежит внутри окружности основания конуса K_i. Когда окончание проекции вектора $\vec{C}_i$ попадает в заштрихованную область вне окружности основания конуса K_i, происходит «прокол» конуса.

Покажем, что с ростом числа итераций i «прокол» конуса прекратится. Так как вектор $\vec{C}_i$ всегда содержит вертикальную составляющую не менее $\frac{r}{|L|}$, то высота конуса K_i растет с каждой итерацией алгоритма. Угол между векторами $\vec{L}$ и $\vec{A}_i$ больше Θ (в противном случае алгоритм останавливается, поскольку решение найдено). Таким образом, радиус основания конуса K_i увеличивается неограниченно.

С увеличением радиуса основания конуса K_i вся заштрихованная область попадает внутрь окружности основания конуса K_i, как показано на рис. 5, и «прокол» конуса прекращается.

Таким образом, «прокол» конуса может произойти конечное число раз, после чего вектор коррекции $\vec{C}_i$ целиком будет лежать внутри конуса K_i, а окончание вектора коррекции всегда будет попадать внутрь круга фиксированного радиуса. С ростом числа итераций высота конуса K_i будет увеличиваться неограниченно, минимум на $\frac{r}{|L|}$ с каждой итерацией (см. рис. 3). Вместе с высотой конуса K_i будет расти радиус основания конуса допустимых решений Q, минимум на $\frac{r}{|L|}\operatorname{tg}\Theta$ с каждой итерацией.

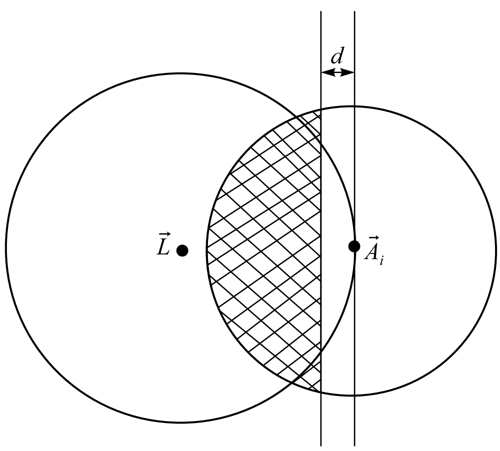

Рис. 4. Проекция на плоскость основания конуса K_i
Fig. 4. Projection onto the plane of the base of the cone K_i

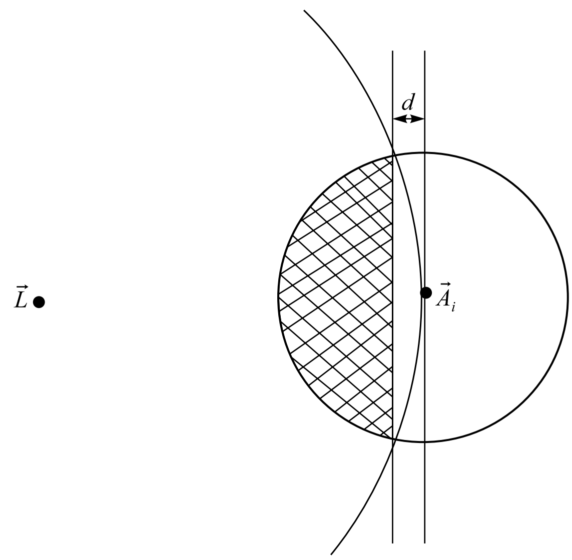

Рис. 5. Проекция на плоскость основания конуса K_i при увеличении радиуса
Fig. 5. Projection onto the plane of the base of the cone with increasing radius

Итак, начиная с некоторого конечного числа шагов алгоритма, все векторы $\vec{A}_i$ будут лежать в вертикальном цилиндре, расположенном внутри конуса допустимых решений, имеющего своей осью вектор $\vec{L}$. Теорема 2 доказана.

Как следует из доказательства, алгоритм сходится при использовании и коэффициентов роста, и коэффициентов возрастания для первичной аппроксимации коэффициентов линейной формы.

Заключение

Таким образом, задача восстановления аналитического задания пороговой функции усложнения при неполных данных может быть успешно решена с помощью геометрического алгоритма характеризации частично известной пороговой *k*-значной функции. В результате будет построена некоторая пороговая функция, совпадающая с частично известной пороговой *k*-значной функцией во всех точках множества *M*.

Библиографические ссылки

1. Бурделёв АВ, Никонов ВГ. О новом алгоритме характеризации *k*-значных пороговых функций. *Computational Nanotechnology.* 2017;1:7–14.
2. Бурделев АВ. О сходимости нового алгоритма характеризации *k*-значных пороговых функций. *Прикладная дискретная математика.* 2018;39:107–115. DOI: 10.17223/20710410/39/10.
3. Бурделёв АВ, Никонов ВГ. О построении аналитического задания *k*-значной пороговой функции. *Computational Nanotechnology.* 2015;2:5–13.
4. Никонов ВГ, Никонов НВ. Особенности пороговых представлений *k*-значных функций. *Труды по дискретной математике.* 2008;11(1):60–85.
5. Минский М, Пейперт С. *Персептроны.* Гимельфарб ГЛ, Шарыпанов ВМ, переводчики; Ковалевский ВА, редактор. Москва: Мир; 1971. 261 с.

References

1. Burdeliov AV, Nikonov VG. About the new algorithm of characterization of *k*-valued threshold functions. *Computational Nanotechnology.* 2017;1:7–14. Russian.
2. Burdelev AV. Convergence of an iterative algorithm for computing parameters of multi-valued threshold functions. *Prikladnaya diskretnaya matematika.* 2018;39:107–115. Russian. DOI: 10.17223/20710410/39/10.
3. Burdeliov AV, Nikonov VG. About construction of analytical definition of *k*-valued threshold function. *Computational Nanotechnology.* 2015;2:5–13. Russian.
4. Nikonov VG, Nikonov NV. [Features of threshold representations of *k*-valued functions]. *Trudy po diskretnoi matematike.* 2008; 11(1):60–85. Russian.
5. Minsky M, Papert S. *Perceptrons: an introduction to computational geometry.* Cambridge: MIT Press; 1969. VI, 258 p.
Russian edition: Minsky M, Papert S. *Perseptrony.* Gimel'farb GL, Sharypanov VM, translators; Kovalevskii VA, editor. Moscow: Mir; 1971. 261 p.

Получена 04.05.2023 / исправлена 25.10.2023 / принята 27.10.2023.
Received 04.05.2023 / revised 25.10.2023 / accepted 27.10.2023.