УДК 512.55

А.В. Бурделев, В.Г. Никонов, И.И. Лапиков

РАСПОЗНАВАНИЕ ПАРАМЕТРОВ УЗЛА ЗАЩИТЫ ИНФОРМАЦИИ, РЕАЛИЗОВАННОГО ПОРОГОВОЙ K-ЗНАЧНОЙ ФУНКЦИЕЙ

Бурделев А.В., Никонов В.Г., Лапиков И.И. **Распознавание параметров узла защиты информации, реализованного пороговой k-значной функцией.**
Аннотация. В статье рассматриваются некоторые подходы к распознаванию параметров пороговых k-значных функций, которые могут быть использованы для построения узлов обработки и защиты информации. Основное внимание сосредоточено на проблеме доказательства принадлежности некоторой k-значной функции к классу пороговых. Для решения этого вопроса предлагается использовать вводимые коэффициенты роста и возрастания, с помощью которых процедурно аппроксимируются коэффициенты линейной формы k-значной пороговой функции. На ряду с предложенным аналитическим подходом в статье рассматривается алгоритмический метод, основанный на сведении задачи нахождения порогового представления k-значной функции к системе линейных неравенств, для решения которой применяется модифицированный метод эллипсоидов Хачияна. На основании экспериментов проводится сравнительный анализ предложенных методов.
Ключевые слова: пороговая k-значная функция, пороговая логика, метод эллипсоидов, характеризация пороговой функции.

Burdeljov A.V., Nikonov V.G., Lapikov I.I. **Recognizing Parameters of the Information Security Unit Implemented by the Threshold K-Valued Function.**
Abstract. This article discusses some approaches to the recognition of the parameters of the threshold k-valued functions, which can be used for building information processing and security units. The main focus is put on the issue of proving k-valued function belonging to the threshold class. For solving this problem it is proposed to use the input coefficients of expansion and increase. With the help of the latter, the coefficients of linear forms of the k-valued threshold function are procedurally approximated. Along with the proposed analytical approach, the article discusses an algorithmic method based on reducing the problem of finding a threshold representation of k-valued functions to the system of linear inequalities, for the solution of which the ellipsoid method, modified by Khachiyan, is applied. The comparative analysis of the proposed methods is carried out based on experiments.
Keywords: threshold k-valued function; threshold logic; ellipsoid method; the characterization of threshold functions.

1. Введение. В настоящее время наблюдается постоянное расширение круга задач, относящихся к сфере информационной безопасности. Прежде всего, это связано с увеличением объемов перерабатываемой информации и ростом быстродействия передающих каналов связи. Поэтому особый интерес представляет переход от битовых преобразований к преобразованиям в k-значной логике. Соответственно, возникает потребность построения узлов защиты информации в k-значной логике. С другой стороны, актуальным направлением развития современных вычислительных технологий является использование

бионических принципов моделирования нейронных сетей живых организмов, что привело к построению так называемых нейрокомпьютеров. Базовыми элементами нейрокомпьютера являются формальные нейроны, функционирование которых описывается пороговыми функциями – булевыми или, как показали последующие исследования, k-значными [6]. Переработка информации в нейросетях делает актуальным построение непосредственно в нейробазисе систем защиты информации, для которых основным узлом усложнения является пороговая функция. Определение параметров таких систем информационной безопасности составляет важнейшую задачу их анализа. Это же относится и к нахождению аналитического задания функции, реализующих преобразования в этих системах. Рассматриваемая в статье задача распознавания параметров пороговой функции относится к этому классу. Здесь необходимо подчеркнуть, что нахождение параметрического задания пороговой функции выходит за рамки исключительно прикладной задачи информационной безопасности. Эта задача является одной из важнейших и актуальных в целом в пороговой логике и ей в разных постановках посвящено большое число известных работ [1, 3, 12, 15, 16]. В тоже время подходы к ее постановке и решению, рассмотренные в данной статье, являются новыми. Во-первых, в большинстве известных работ внимание авторов было сосредоточено на построении одной плоскости, разделяющей рассматриваемое множество на два подмножества, как в булевом, так и в k-значном случаях, здесь же изучается представление в целом k-значной пороговой функции с помощью системы параллельных плоскостей. Во-вторых, в статье предложено два принципиально отличающихся приема решения поставленной задачи: параметрический, основанный на использовании коэффициентов роста и возрастания и алгоритмический, при котором задача сводится к системе линейных неравенств в действительной области, для решения которой применяется метод эллипсоидов Хачияна.

2. Задача характеризации пороговой функции. Важной задачей пороговой логики является задача распознавания принадлежности функции к классу пороговых. В случае ее положительного решения, возникает необходимость нахождения коэффициентов линейной формы и порога. Обе эти задачи взаимосвязаны, но, несмотря на простоту формулировки, являются достаточно сложными и рассматривались многими авторами [4, 5, 8, 17, 18]. В то же время подходы, предлагаемые в статье, представляются новыми и могут вызвать интерес у специалистов в данной научной области.

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 a 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.

Одним из подходов к решению задачи нахождения коэффициентов линейной формы и порога в булевом случае является использование коэффициентов характеристического вектора функции в качестве модели первого приближения для коэффициентов $a_1,\ldots,a_n$ искомого порогового задания

$$a_1x_1+a_2x_2+\ldots+a_nx_n \ge b$$

булевой функции $f(x_1,\ldots,x_n)$.

Определение 2. Пусть функция $f(x)$, представлена в базисе $\{-1,1\}$. Упорядоченный набор весов $c_0,c_1,\ldots,c_n$, где

$$c_i=\sum_{x\in V_2^n} x_i f(x),\ i=\overline{1,n},$$

$$c_0=\sum_{x\in V_2^n} f(x)$$

называется характеристическим вектором c функции $f(x)$.

Коэффициенты характеристического вектора $c_i, i=\overline{1,n}$ можно трактовать как параметры близости функции $f(x)$ к функциям x_i.

Определение 3. Будем говорить, что линейная форма $L(x_1,\ldots,x_n)=a_1x_1++a_2x_2+\ldots+a_nx_n$ дает точное разделение областей значений функции $f^k(\varepsilon_1,\ldots,\varepsilon_n)$, если для любого $i=\overline{0,k-2}$ выполняется строгое неравенство:

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

В случае если построенная с помощью коэффициентов $(a_1,\ldots,a_n)$ линейная форма дает точное разделение областей зна-

чений функции $f^k(\varepsilon_1,\ldots,\varepsilon_n)$, границы $b_0, b_1, \ldots, b_k$ можно определить, например, следующим способом:

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

$$b_k = \max_{f^k(\varepsilon_1,\ldots,\varepsilon_n)=k} \{a_1\varepsilon_1 + \ldots + a_n\varepsilon_n\} + 1. \quad (2)$$

Подчеркнем, что коэффициенты характеристического вектора используются для первого приближения коэффициентов $a_1, a_2, \ldots, a_n$ искомого порогового задания:

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n \geq b.$$

В работе [2] изложены итеративные алгоритмы вычисления коэффициентов $a_1, a_2, \ldots, a_n$ с помощью коэффициентов $c_1, \ldots, c_n$ характеристического вектора функции: метод минимизации функционала [2, глава 3] и итеративный метод синтеза порогового элемента [2, глава 4]. Можно сделать вывод, что задача нахождения параметров пороговой булевой функции является объективно более сложной математической задачей, чем задача определение принадлежности функции классу пороговых функций, и сводится к итеративной процедуре.

3. Параметры близости и отличия k-значных функций. При рассмотрении вопроса построения порогового представления k-значной пороговой функции первой проблемой является выбор меры близости исходной функции к функциям x_i. Таких мер близости двух k-значных функций может быть предложено несколько.

Определение 4. Для функции $f^k(x_1,\ldots,x_n)$ мультипликативным коэффициентом переменной x_i называется величина:

$$\xi_{x_i} = \sum_{(x_1,\ldots,x_n)} (x_i f^k(x_1,\ldots,x_n)).$$

Определение 5. Для функции $f^k(x_1,\ldots,x_n)$ разностным коэффициентом переменной x_i называется величина:

$$\eta_{x_i} = \sum_{(x_1,\ldots,x_n)} \left| x_i - f^k(x_1,\ldots,x_n) \right|.$$

Определение 6. Для функции $f^k(x_1,\ldots,x_n)$ квадратичным коэффициентом переменной x_i называется величина:

$$\delta_{x_i} = \sum_{(x_1,\ldots,x_n)} \left(x_i - f^k\left(x_1,\ldots,x_n\right)\right)^2.$$

Определение 7. Для функции $f^k\left(x_1,\ldots,x_n\right)$ коэффициентом роста по переменной x_i называется величина:

$$\Delta_{x_i} = \sum_{(x_1,\ldots,x_{i-1},x_{i+1}\ldots,x_n)} \sum_{\varepsilon=0}^{k-2} (f^k(x_1,\ldots,x_{i-1},\varepsilon+1,x_{i+1},\ldots,x_n) - f^k(x_1,\ldots,x_{i-1},\varepsilon,x_{i+1},\ldots,x_n)).$$

Определение 8. Для функции $f^k\left(x_1,\ldots,x_n\right)$ коэффициентом возрастания по переменной x_i называется величина:

$$\lambda_{x_i} = \sum_{(x_1,\ldots,x_{i-1},x_{i+1}\ldots,x_n)} \sum_{\varepsilon=0}^{k-2} \sum_{\varepsilon=l+1}^{k-1} (f^k(x_1,\ldots,x_{i-1},\varepsilon+1,x_{i+1},\ldots,x_n) - f^k(x_1,\ldots,x_{i-1},l,x_{i+1},\ldots,x_n)).$$

Все введенные выше коэффициенты характеризуют меру близости функций $f^k\left(x_1,\ldots,x_n\right)$ и x_i, однако для задачи нахождения аналитического представления k-значной пороговой функции они подходят с разной эффективностью. Так, для некоторых пороговых k-значных функций коэффициенты роста и возрастания приводят к прямому нахождению коэффициентов $a_1,\ldots,a_n$, в то время как мультипликативные, разностные и квадратичные коэффициенты не дают построения разделяющей плоскости. Рассмотрим пример.

Пример 1. Рассмотрим функцию $f^3\left(x_1,x_2,x_3\right):\mathbb{Z}_3\times\mathbb{Z}_3\times$ $\times\mathbb{Z}_3\to\mathbb{Z}_3$, графически представленную на рисунке 1, которая задается линейной формой $L\left(x_1,x_2,x_3\right) = \ = 3x_1+2x_2+x_3$ и системой порогов следующим образом:

$$f^3\left(x_1,x_2,x_3\right)=0 \Leftrightarrow 0\le L\left(x_1,x_2,x_3\right)<5,$$
$$f^3\left(x_1,x_2,x_3\right)=1 \Leftrightarrow 5\le L\left(x_1,x_2,x_3\right)<8,$$
$$f^3\left(x_1,x_2,x_3\right)=2 \Leftrightarrow 8\le L\left(x_1,x_2,x_3\right)<13.$$

Для данной функции введенные выше коэффициенты равны:

1. Мультипликативные коэффициенты: $\xi_{x_1}=41$, $\xi_{x_2}=35$, $\xi_{x_3}=31$.
2. Разностные коэффициенты: $\eta_{x_1}=8$, $\eta_{x_1}=16$, $\eta_{x_3}=20$.
3. Квадратичные коэффициенты: $\delta_{x_1}=8$, $\delta_{x_2}=20$, $\delta_{x_3}=28$.

4. Коэффициенты роста: $\Delta_{x_1} = 14$, $\Delta_{x_2} = 8$, $\Delta_{x_3} = 4$.
5. Коэффициенты возрастания: $\lambda_{x_1} = 28$, $\lambda_{x_2} = 16$, $\lambda_{x_3} = 8$.

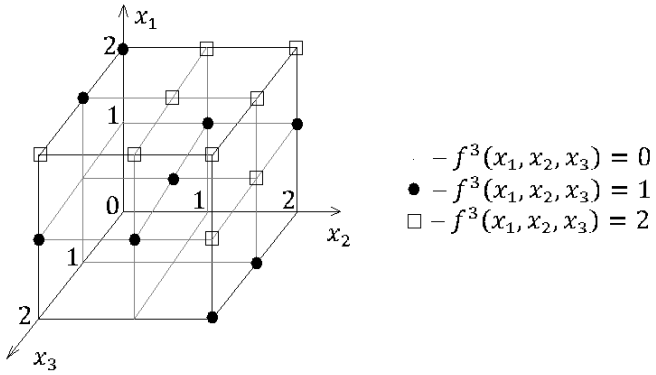

Рис. 1. Графическое представление функции $f^3(x_1, x_2, x_3)$

Коэффициенты роста и коэффициенты возрастания сразу дают разделяющую плоскость.

Действительно, составив из коэффициентов роста функции $f^3(x_1, x_2, x_3)$ линейную форму $L'(x_1, x_2) = 14x_1 + 8x_2 + 4x_3$, получаем точное разделение областей значений функции $f^3(x_1, x_2, x_3)$. После вычисления границ по формулам (1), (2) $b_0 = 0$, $b_1 = 20$, $b_2 = 34$, $b_3 = 53$, приведенным выше способом, получим реализацию функции $f^3(x_1, x_2, x_3)$:

$$f^3(x_1, x_2, x_3) = 0 \Leftrightarrow 0 \le L'(x_1, x_2, x_3) < 20,$$
$$f^3(x_1, x_2, x_3) = 1 \Leftrightarrow 20 \le L'(x_1, x_2, x_3) < 34,$$
$$f^3(x_1, x_2, x_3) = 2 \Leftrightarrow 34 \le L'(x_1, x_2, x_3) < 53.$$

Составив из коэффициентов возрастания функции $f^3(x_1, x_2, x_3)$ линейную форму $L''(x_1, x_2) = 28x_1 + 16x_2 + 8x_3$, также получаем точное разделение областей значений функции $f^3(x_1, x_2, x_3)$. После вычисления границ $b_0 = 0$, $b_1 = 40$, $b_2 = 68$, $b_3 = 103$, приведенным выше способом, получаем реализацию функции $f^3(x_1, x_2, x_3)$:

$$f^3(x_1,x_2,x_3)=0 \Leftrightarrow 0 \le L''(x_1,x_2,x_3) < 40,$$
$$f^3(x_1,x_2,x_3)=1 \Leftrightarrow 40 \le L``(x_1,x_2,x_3) < 68,$$
$$f^3(x_1,x_2,x_3)=2 \Leftrightarrow 68 \le L``(x_1,x_2,x_3) < 103.$$

Таким образом, вычисление коэффициентов роста и возрастания функции $f^3(x_1,x_2,x_3)$ сразу решает задачу характеризации. При этом мультипликативные, разностные и квадратичные коэффициенты не дают построения разделяющей плоскости. Таким образом, пример 1 показывает, что в дальнейшем целесообразно рассматривать только коэффициенты роста и возрастания.

4. Нахождение порогового представления k-значной функции с помощью коэффициентов роста и возрастания. Оставшиеся в рассмотрении коэффициенты роста и возрастания не одинаково эффективно характеризуют пороговые k-значные функции. Так, использование коэффициентов роста не всегда приводит к непосредственному нахождению коэффициентов $a_1,\ldots,a_n$.

*Пример 2***.** Рассмотрим функцию $f^4(x_1,x_2):\mathbb{Z}_4\times\mathbb{Z}_4\to\mathbb{Z}_4$, графически представленную на рисунке 2, которая задается линейной формой $L(x_1,x_2)=2x_1+5x_2$ и системой порогов следующим образом:

$$f^4(x_1,x_2)=0 \Leftrightarrow 0 \le L(x_1,x_2) < 6,$$
$$f^4(x_1,x_2)=1 \Leftrightarrow 6 \le L(x_1,x_2) < 11,$$
$$f^4(x_1,x_2)=2 \Leftrightarrow 11 \le L(x_1,x_2) < 17,$$
$$f^4(x_1,x_2)=3 \Leftrightarrow 17 \le L(x_1,x_2).$$

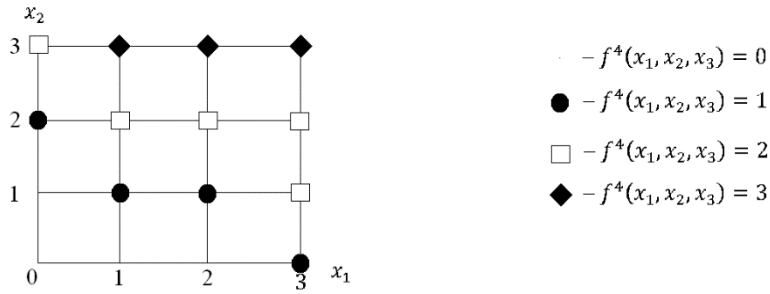

Рис. 2. Графическое представление функции $f^4(x_1,x_2)$

Для данной функции коэффициенты роста и возрастания равны:

1. Коэффициенты роста: $\Delta_{x_1}=5$, $\Delta_{x_2}=10$.
2. Коэффициенты возрастания: $\lambda_{x_1}=15$, $\lambda_{x_2}=33$.

Построенная с помощью коэффициентов роста $\Delta_{x_1}=5$, $\Delta_{x_2}=10$ линейная форма $L'(x_1,x_2)=5x_1+10x_2$ не дает точное разделение областей значений функции $f^4(x_1,x_2)$:

$$\max_{f^4(x_1,x_2)=2}\{5x_1+10x_2\}=L'(3,2)=35=L'(1,3)=\min_{f^4(x_1,x_2)=3}\{5x_1+10x_2\}.$$

Построенная с помощью коэффициентов возрастания $\lambda_{x_1}=15$ и $\lambda_{x_1}=33$ линейная форма $L''(x_1,x_2)=15x_1+33x_2$ дает точное разделение областей значений функции $f^3(x_1,x_2)$: вычислив границы $b_0=0$, $b_1=45$, $b_2=78$, $b_3=114$, $b_4=145$, получаем реализацию функции $f^3(x_1,x_2)$:

$$f^4(x_1,x_2)=0\Leftrightarrow 0\le L''(x_1,x_2)<45,$$
$$f^4(x_1,x_2)=1\Leftrightarrow 45\le L''(x_1,x_2)<78,$$
$$f^4(x_1,x_2)=2\Leftrightarrow 78\le L''(x_1,x_2)<114,$$
$$f^4(x_1,x_2)=3\Leftrightarrow 114\le L''(x_1,x_2)<145.$$

Из примера 2 видно, что линейная форма, построенная с помощью коэффициентов роста, не всегда дает точное разделение областей значений функции. На основании примера можно заключить, что при нахождении линейной формы предпочтение стоит отдать использованию коэффициентов возрастания, которые дают более точное приближение коэффициентов линейной формы.

Так как в булевом случае подобная задача решается итеративно [см. 2], то следует ожидать, что и коэффициенты возрастания также не всегда дадут точное разделение областей значений функции. Это подтверждает следующий пример.

Пример 3. Рассмотрим функцию $f^4(x_1,x_2):\mathbb{Z}_4\times\mathbb{Z}_4\to\mathbb{Z}_4$, графически представленную на рисунке 3, которая задается линейной формой $L(x_1,x_2)=5x_1+x_2$ и системой порогов следующим образом:

$$f^4(x_1,x_2)=0 \Leftrightarrow 0 \le L(x_1,x_2) < 15{,}5,$$
$$f^4(x_1,x_2)=1 \Leftrightarrow 15{,}5 \le L(x_1,x_2) < 16{,}5,$$
$$f^4(x_1,x_2)=2 \Leftrightarrow 16{,}5 \le L(x_1,x_2) < 17{,}5,$$
$$f^4(x_1,x_2)=3 \Leftrightarrow 17{,}5 \le L(x_1,x_2).$$

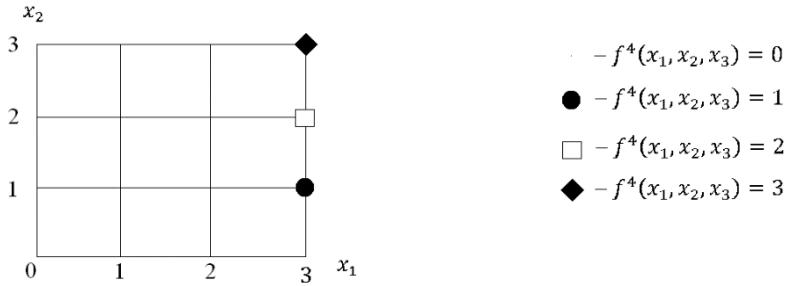

Рис. 3. Графическое представление функции $f^4(x_1,x_2)$.

Коэффициенты роста и возрастания данной функции равны:

1. Коэффициенты роста: $\Delta_{x_1}=6$, $\Delta_{x_2}=3$.
2. Коэффициенты возрастания: $\lambda_{x_1}=18$, $\lambda_{x_2}=10$.

Линейная форма $L'(x_1,x_2)=6x_1+3x_2$, полученная с помощью коэффициентов роста, не дает точное разделение областей значений функции $f^4(x_1,x_2)$:

$$\min_{f^4(x_1,x_2)=1}\{6x_1+3x_2\}=L'(3,1)=21=L'(2,3)=\max_{f^4(x_1,x_2)=0}\{6x_1+3x_2\}.$$

Линейная форма $L''(x_1,x_2)=18x_1+10x_2$, полученная с помощью коэффициентов возрастания, также не дает точное разделение областей значений функции $f^4(x_1,x_2)$:

$$\min_{f^4(x_1,x_2)=1}\{18x_1+10x_2\}=L'(3,1)=64<66=L'(2,3)=\max_{f^4(x_1,x_2)=0}\{18x_1+10x_2\}.$$

Таким образом, ни один из предложенных вариантов трактовки близости или отличия двух k-значных функций для характеризации пороговых функций не дает точное разделение областей значений функции. При этом в роли первичного приближения коэффициентов линейной формы целесообразно использовать коэффициенты возрас-

тания. В дальнейшем аналогично булевому случаю необходимо введение итеративной процедуры.

5. Применение итеративной процедуры для нахождения коэффициентов линейной формы. Для характеризации k-значных пороговых функций целесообразно вычислять первичное приближение коэффициентов линейной формы с помощью коэффициентов возрастания. Далее необходимо введение итеративной процедуры для нахождения коэффициентов линейной формы, дающей точное разделение. На идейном уровне можно предложить следующую процедуру.

Пусть построенная с помощью коэффициентов роста линейная форма $L(x_1,\ldots,x_n)$ не дает точное разделение областей значений функции $f^k(x_1,\ldots,x_n)$, то есть существует $i\in\overline{0,k-2}$ такое, что выполняется неравенство:

$$\max_{f^k(\varepsilon_1,\ldots,\varepsilon_n)=i}\{a_1\varepsilon_1+\ldots+a_n\varepsilon_n\}\geq \min_{f^k(\varepsilon_1,\ldots,\varepsilon_n)=i+1}\{a_1\varepsilon_1+\ldots+a_n\varepsilon_n\}.$$

Рассмотрим точки:

$$A=(u_1,\ldots,u_n)\in M_i=\{x: f(x)=i\} \text{ и}$$
$$B=(v_1,\ldots,v_n)\in M_{i+1}=\{x: f(x)=i+1\},$$

такие, что линейная форма $L(x_1,\ldots,x_n)$ принимает на них максимальное значение из множества M_i и минимальное значение из множества M_{i+1} соответственно. Таких точек может быть несколько. Для них выполняется неравенство:

$$L(A)\geq L(B).$$

Уравнение:

$$L(x_1,\ldots,x_n)=b,\quad b\in\mathbb{R}$$

задает гиперплоскость, рассекающую n-мерный куб (рисунок 4).

Предлагаемая процедура корректировки должна наклонить множество гиперплоскоскостей, задающихся линейной формой $L(x_1,\ldots,x_n)$ так, чтобы после смещения гиперплоскость отсекала точки A и B в ином порядке, чем до корректировки.

Наклон «в нужную сторону» можно задать прибавлением к линейной форме $L(x_1,\ldots,x_n)$ двух линейных форм, соответствующих двум рассматриваемым точкам A и B. Эти две линейные формы со-

ставляются по координатам точек A и B, и берутся с разными знаками: в первую линейную форму подставляются координаты точки B, во вторую – координаты точки A с отрицательными знаками:

$$L'(x_1,\ldots,x_n) = L(x_1,\ldots,x_n) + v_1x_1 + \ldots + v_nx_n - u_1x_1 - \ldots - u_nx_n\,.$$

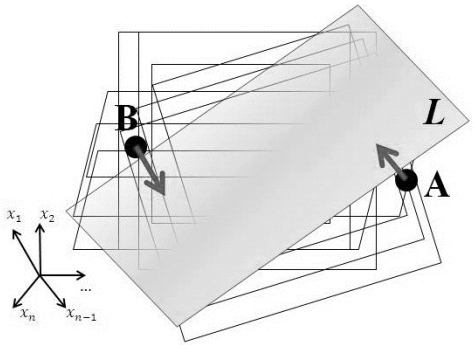

Рис. 4. Графическое представление рассечения n-мерного куба гиперплоскостью

Для полученной таким образом линейной формы $L'(x_1,\ldots,x_n)$ вычисляются ее значения на множествах:

$$M_i = \{x : f(x) = i\},\ \ i \in \overline{0,k-1},$$

и сравнением соответствующих минимальных и максимальных значений определяется, дает ли она точное разделение областей значений функции $f^k(x_1,\ldots,x_n)$. Если она не дает точное разделение, то процедура повторяется. Если после корректировки линейная форма дает точное разделение областей значений функции $f^k(x_1,\ldots,x_n)$, то алгоритм заканчивает работу: коэффициенты линейной формы найдены.

Возможно, что в случае зацикливания алгоритма необходимо будет прибавлять корректирующие линейные формы с коэффициентами c_1 и c_2 меньшими единицы:

$$L'(x_1,\ldots,x_n) = L(x_1,\ldots,x_n) + c_1(v_1x_1 + \ldots + v_nx_n) - c_2(u_1x_1 - \ldots - u_nx_n)\,.$$

Пример 6. Рассмотрим коррекцию линейной формы:

$$L(x_1,x_2) = 18x_1 + 10x_2, \qquad (3)$$

полученную с помощью коэффициентов возрастания в примере 5. Точному разделению мешают точки (3,1) и (2,3). Прибавим соответствующие линейные формы в (3). Получим:

$$L(x_1,x_2)=18x_1+10x_2+3x_1+1x_2-2x_1-3x_2=19x_1+8x_2.$$

Данная линейная форма дает точное разделение областей значений функции $f^4(x_1,x_2)$ и исправляет нарушение разделения в корректируемых точках:

$$\min_{f^4(x_1,x_2)=1}\{19x_1+8x_2\}=L(3,1)=65>62=L(2,3)==\max_{f^4(x_1,x_2)=0}\{19x_1+8x_2\}.$$

6. Применение метода эллипсоидов Хачияна для нахождения коэффициентов линейной формы. 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:

$$f^k(x_1,\ldots,x_n)=i\Leftrightarrow b_i\le a_1\varepsilon_1+a_2\varepsilon_2+\ldots+a_n\varepsilon_n<b_{i+1}, \qquad (4)$$

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 (4) для всех точек ($\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n$) формирует систему:

$$\begin{cases} b_0\le a_1\varepsilon_1^{(1)}+a_2\varepsilon_2^{(1)}+\ldots+a_n\varepsilon_n^{(1)}<b_1,\\ b_{k-1}\le a_1\varepsilon_1^{(k^n)}+a_2\varepsilon_2^{(k^n)}+\ldots+a_n\varepsilon_n^{(k^n)}<b_k. \end{cases} \qquad (5)$$

с целочисленными коэффициентами и действительными неизвестными. Полученная система (5) в точности соответствует системе линейных неравенств, рассмотренных Хачияном [9]. Для решения (5) им был предложен полиномиальный алгоритм эллипсоидов, который за известное число шагов дает ответ: совместима система (5) или нет. В случае совместимости определяет решение. Алгоритм используется для решения систем из $m \geq 2$ линейных неравенств относительно $n \geq 2$ действительных неизвестных $x_1, x_2, ..., x_n$:

$$\begin{cases} a_{11}x_1 + ... + a_{1n}x_n \leq b_1, \\ \quad ... \\ a_{m1}x_1 + ... + a_{mn}x_n \leq b_m, \end{cases} \tag{6}$$

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

$$L = \left[\sum_{i,j=1}^{m,n} \log_2 (|a_{i,j}| + 1) + \sum_{i=1}^{m} \log_2 (|b_i| + 1) + \log_2 mn \right] + 1, \tag{7}$$

т.е. число символов, необходимых для записи коэффициентов в двоичной системе. Для удобства рассматриваемые в дальнейшем системы запишем в виде (8):

$$A_i x \leq b_i, i = \overline{1, m}, \tag{8}$$

где A_i — строки матрицы коэффициентов системы (6), а b_i — свободные члены.

Методику сведения рассмотрим на примере функции 4-значной логики φ от переменных x_1, x_2, $x_i \in \{0,1,2,3\}$, которая задана таблично (см. Таблицу 1) на всех наборах значений аргументов.

Таблица 1 Табличное задание функции $\varphi(x_1, x_2)$ на всех наборах аргументов

x_1	x_2	$\varphi(x_1, x_2)$	x_1	x_2	$\varphi(x_1, x_2)$
0	0	0	2	0	0
0	1	0	2	1	0
0	2	0	2	2	0
0	3	0	2	3	0
1	0	0	3	0	0
1	1	0	3	1	1
1	2	0	3	2	2
1	3	0	3	3	3

Задача нахождения аналитического представления пороговой функции f от переменных x_1, x_2, $x_i \in \{0,1,2,3\}$ сводится к задаче нахождения линейной формы $L(u_1,u_2) = a_1u_1 + a_2u_2$ и системы порогов b_α таких, что $f(\varepsilon_1,\varepsilon_2) = \alpha \Leftrightarrow b_\alpha < L(\varepsilon_1,\varepsilon_2) \le b_{\alpha+1}, \alpha \epsilon \{0,1,2,3\}$.

Причем для $\alpha = 0$ и $\alpha = 3$ пороговое ограничение линейной формы $L(\varepsilon_1,\varepsilon_2)$ будет иметь односторонний характер, то есть вся система ограничений будет иметь вид:

$$\begin{cases} f(\varepsilon_1,\varepsilon_2) = 0 \Leftrightarrow L(\varepsilon_1,\varepsilon_2) \le b_0, \\ f(\varepsilon_1,\varepsilon_2) = 1 \Leftrightarrow b_0 < L(\varepsilon_1,\varepsilon_2) \le b_1, \\ f(\varepsilon_1,\varepsilon_2) = 2 \Leftrightarrow b_1 < L(\varepsilon_1,\varepsilon_2) \le b_2, \\ f(\varepsilon_1,\varepsilon_2) = 3 \Leftrightarrow L(\varepsilon_1,\varepsilon_2) > b_2. \end{cases} \quad (9)$$

Рассмотрим методику формирования системы линейных неравенств с использованием таблицы 1 и системы ограничений (9). Сформируем неравенства для каждого значения функции $\varphi(x_1,x_2)$.

Пусть $\varphi(x_1,x_2) = 0$, тогда получим следующие неравенства:

$0 \le b_0$,
$a_2 \le b_0$,
$2a_2 \le b_0$,
$3a_2 \le b_0$,
$a_1 \le b_0$,
$a_1 + a_2 \le b_0$,
$a_1 + 2a_2 \le b_0$,
$a_1 + 3a_2 \le b_0$,
$2a_1 \le b_0$,
$2a_1 + a_2 \le b_0$,
$2a_1 + 2a_2 \le b_0$,
$2a_1 + 3a_2 \le b_0$,
$3a_1 \le b_0$.

Для $\varphi(x_1,x_2) = 1$, получим ограничение:

$$b_0 < 3a_1 + a_2 \le b_1 \Leftrightarrow \begin{cases} 3a_1 + a_2 \le b_1, \\ -3a_1 - a_2 + b_0 \le -1. \end{cases}$$

Для $\varphi(x_1,x_2) = 2$, получим ограничение:

$$b_1 < 3a_1 + 2a_2 \le b_2 \Leftrightarrow \begin{cases} 3a_1 + 2a_2 \le b_2, \\ -3a_1 - 2a_2 + b_1 \le -1. \end{cases}$$

Для $\varphi(x_1, x_2) = 3$, получим ограничение:

$$3a_1 + 3a_2 > b_2 \Leftrightarrow 3a_1 + 3a_2 \geq b_2 + 1.$$

Таким образом, приводя все неравенства к виду (8), получим систему линейных неравенств (10) с 5 неизвестными a_1, a_2, b_0, b_1, b_2.

$$\begin{cases} -b_0 \leq 0, \\ a_2 - b_0 \leq 0, \\ 3a_2 - b_0 \leq 0, \\ a_1 - b_0 \leq 0, \\ a_1 + a_2 - b_0 \leq 0, \\ a_1 + 2a_2 - b_0 \leq 0, \\ a_1 + 3a_2 - b_0 \leq 0, \\ 2a_1 - b_0 \leq 0, \\ 2a_1 + a_2 - b_0 \leq 0, \\ 2a_1 + 2a_2 - b_0 \leq 0, \\ 2a_1 + 3a_2 - b_0 \leq 0 \\ 3a_1 - b_0 \leq 0, \\ 3a_1 + a_2 - b_1 \leq 0, \\ -3a_1 - a_2 + b_0 \leq -1, \\ 3a_1 + 2a_2 - b_2 \leq 0, \\ -3a_1 - 2a_2 + b_1 - 1, \\ -3a_1 - 3a_2 + b_2 \leq -1. \end{cases} \quad (10)$$

Для решения системы (10) применим модифицированный алгоритм, основанный на методе эллипсоидов Л.Г Хачияна. Модифицируем полиномиальный алгоритм Хачияна, введя дополнительный критерий выхода из алгоритма по отрицательной невязке в центре эллипсоида, полученного на очередной итерации алгоритма. Этот критерий является корректным поскольку $\theta(x_k) = \max\limits_{i=1\ldots m} \left\{ A_i^T x_k - b_i \right\}$ и если $\theta(x_k) \leq 0$, то очевидно, что все неравенства системы вида (1) выполняются и центр очередного эллипсоида x_k попадает в многогранник решений системы (1). Если исходная система (1) несовместна, то выход по введенному критерию невозможен, поскольку коэффициент

невязки $\theta(x_k)$ будет положительным на всех $6n^2L$ итерациях, где n — количество неизвестных в системе (1), L — длина входа системы [9].

Следовательно, данная модификация никак не повлияет на корректность работы всего алгоритма в целом и все леммы из [7] так же будут верны. По описанной методике алгоритм находит решение системы линейных неравенств (10) за 46 итераций. Центр эллипсоида на 46 итерации определяется:

$$x_{45} = \begin{pmatrix} 3.61960930519009E+20 \\ 1.47740024806186E+20 \\ 1.18037089474546E+21 \\ 1,3317378744761E+21 \\ 1,42000658030312E+21 \end{pmatrix},$$

которая соответствует вектору неизвестных $\overline{X} = (a_1, a_2, b_0, b_1, b_2)$. Произведем округление и сокращение на 10^{20} и запишем окончательное решение $\overline{X}_{оконч} = (3.62,\ 1.48,\ 11.8, 13.31, 14.22)$.

Таким образом, искомая пороговая функция f описывается линейной формой:

$$L(u_1, u_2) = 3.62u_1 + 1.48u_2$$

и системой порогов $b_i = (b_0, b_1, b_2) = (11.8, 13.31, 14.22)$.

Непосредственная проверка для всех наборов значений аргументов подтверждает, что найденное аналитическое представление пороговой функции заданного таблично отображения в k-значной области является корректным. Приведенная методика может быть обобщена для нахождения аналитического представления всех таблично заданных функции k-значной логики. Причем, если мы с достаточной степенью достоверности сможем утверждать о несовместности полученной системы линейных неравенств, то можно будет предположить, что заданная таблично функция k-значной логики не имеет порогового представления.

7. Заключение. Предложенные в данной статье подходы к распознаванию параметров k-значной пороговой функции являются новыми, а то обстоятельство, что все они приводят к решению, позволяет дать им в целом положительную оценку. Их более глубокое изучение и

проведение сопоставительного анализа определяют направление для дальнейших исследований в данной области.

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. 344 с.
3. *Зуев А.Ю.* Пороговые функции и пороговые представления булевых функций // Математические вопросы кибернетики. 1994. № 5. С. 5–61.
4. *Никонов В.Г.* Пороговые представления булевых функций // Обозрение прикл. и промышл. матем. 1994. Вып. 1. № 3. С. 458–545.
5. *Никонов В.Г., Никонов Н.В.* Особенности пороговых представлений k-значных функций // Труды по дискр. матем. 2008. Вып. 11. №. 1. С. 60–85.
6. *Вальцев В.Б., Григорьев В.Р., Никонов В.Г.* Некоторые структурные принципы организации высших функций мозга // Нейрокомпьютер как основа мыслящих ЭВМ. 1993. С. 38–46.
7. *Хачиян Л.Г.* Полиномиальные алгоритмы в линейном программировании // ЖВМиМФ. 1980. Вып. 20. № 1. С. 51–68.
8. *Золотых Н.Ю.* Расшифровка пороговой функции, заданной расширенным оракулом // Вестник Нижегородского университета им. Н.И. Лобачевского. 2012. № 3(1). С. 175–178.
9. *Хачиян Л.Г.* Полиномиальный алгоритм в линейном программировании // Докл. АН СССР. 1978. Вып. 244. № 5. С. 1093–1096.
10. *Кудрявцев В.Б.* Теория тестового распознавания // Дискретная математика. 2006. Вып. 18. № 3. С. 3–34.
11. *Winder R.O.* The status of threshold logic // RCA Review. 1969. vol. 30. no. 1. pp. 62–84.
12. *Золотых Н.Ю.* Расшифровка пороговых и близких к ним функций многозначной логики // Автореферат диссертации на соискание ученой степени канд. физ.-мат. наук. Нижний Новгород: Нижегородский гос. университет им. Н. И. Лобачевского. 1998. 12 с.
13. *Загоруйко Н.Г.* Прикладные методы анализа данных и знаний // Новосибирск: ИМ СО РАНю 1999. 270 с.
14. *Золотых Н.Ю.* О пороговых и близких к ним функциях, определенных в целочисленных точках политопа // Дискретный анализ и исследование операций: серия 1. 1998. Вып. 5. № 2. С. 40–54.
15. *Кудрявцев В.Б.* Теория тестового распознавания // Дискретная математика. 2006. Вып. 18. № 3. С. 3–34.
16. *Журавлев Ю.И.* Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики. 1978. №. 33. С. 5–68.
17. *Goldberg P.W.* Learning fixed-dimension linear thresholds from fragmented data // Information and Computation. 2001. vol. 171. no. 1. pp. 98–122.
18. *Irmatov A.A.* Arrangements of hyperplanes and the number of threshold functions // Acta Applicandae Mathematicae. 2001. vol. 68. no. 1–3. pp. 211–226.

References

1. Butakov E.A. *Metody sinteza relejnyh ustrojstv iz porogovyh jelementov* [Methods for synthesis of relay devices of the threshold elements]. M: Jenergija. 1970. 328 p. (In Russ.).

2. Dertouzos M. *Porogovaja logika* [The threshold logic]. M.: Mir. 1967. 344 p. (In Russ.).
3. Zuev A.Ju. [The threshold function and threshold representations of Boolean functions]. *Matematicheskie voprosy kibernetiki – Mathematical problems of cybernetics*. 1994. no. 5. pp. 5–61. (In Russ.).
4. Nikonov V.G. [The threshold representations of Boolean functions]. *Obozrenie prikl. i promyshl. matem. – Review of Applied and Industrial Mathematics.* 1994. vol. 1. no. 3. pp. 458–545. (In Russ.).
5. Nikonov V.G., Nikonov N.V. [Features of threshold representations of k-valued functions]. *Trudy po diskr. matem. – Proceeding on Discrete Mathematics.* 2008. vol. 11. no. 1. pp. 60–85. (In Russ.).
6. Val'cev V.B., Grigor'ev V.R., Nikonov V.G. [Some structural principles of higher brain functions]. *Nejrokomp'juter kak osnova mysljashhih JeVM – Neurocomputer as a basis for thinking computer*. 1993. pp. 38–46. (In Russ.).
7. Hachijan L.G. [Polynomial algorithms in linear programming]. *ZhVMiMF – CMaMPJ*. 1980. vol. 20. no. 1. pp. 51–68. (In Russ.).
8. Zolotyh N.Ju. [Deciphering of threshold functions, given the advanced oracle]. *Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo – Bulletin of the Nizhny Novgorod University. N.I Lobachevsky*. 2012. no. 3(1). pp. 175– 178. (In Russ.).
9. Hachijan L.G. [A polynomial algorithm for linear programming]. *Dokl. AN SSSR – Reports of the AS USSR.* 1978. vol. 244. no. 5. pp. 1093–1096. (In Russ.).
10. Kudrjavcev V.B. [Test recognition theory]. *Diskretnaja matematika – Discrete Math*. 2006. vol. 18. no 3. pp. 3–34. (In Russ.)
11. Winder R.O. The status of threshold logic. *RCA Review.* 1969. vol. 30. no. 1. pp. 62–84.
12. Zolotyh N. Ju. *Rasshifrovka porogovyh i blizkih k nim funkcij mnogoznachnoj logiki*. Avtoreferat dissertacii na soiskanie uchenoj stepeni kand. fiz.-mat. nauk.[Deciphering of threshold and similar functions of many-valued logic. Abstract of the thesis for the degree of Cand. Sci. Sciences]. Nizhnij Novgorod: Nizhegorodskij gos. universitet im. N.I. Lobachevskogo. 1998. 12 p. (In Russ.).
13. Zagorujko N. G. *Prikladnye metody analiza dannyh i znanij* [Applied methods of data analysis and knowledge]. Novosibirsk: IM SO RAN. 1999. 270 p. (In Russ.).
14. Zolotyh N.Ju. [On threshold and nearly threshold functions defined at integer points of a polytope]. *Diskretnyj analiz i issledovanie operacij. Serija 1 – Discrete Analysis and Operations Research: Series 1.* 1998. vol. 5. no. 2. pp. 40–54. (In Russ.).
15. Kudrjavcev V.B. [Test recognition theory]. *Diskretnaja matematika – Discrete Math*. 2006. vol. 18. no. 3. pp. 3–34. (In Russ.)
16. Zhuravlev Ju.I. [On the algebraic approach to solving the problems of recognition and classification]. *Problemy kibernetiki – Problems of Cybernetics*. 1978. vol. 33. pp. 5–68. (In Russ.).
17. Goldberg P.W. Learning fixed-dimension linear thresholds from fragmented data. *Information and Computation*. 2001. vol. 171. no. 1. pp. 98–122.
18. *Irmatov A.A.* Arrangements of hyperplanes and the number of threshold functions. *Acta Applicandae Mathematicae.* 2001. vol. 68. no. 1–3. pp. 211–226.

Бурделев Александр Владимирович — старший преподаватель кафедры математического моделирования и анализа данных факультета прикладной математики и информатики, Белорусский государственный университет (БГУ). Область научных интересов: пороговая логика, построение пороговых функций, распознавание параметров k-значных функций. Число научных публикаций — 3. aburd2011@mail.ru; пр. Независимости, 4, Минск, 220030, Беларусь; р.т.: +375445737505.

Burdeljov Aleksandr Vladimirovich — senior lecturer of mathematical modeling and data analysis department of faculty of applied mathematics and computer science, Belarusian State University (BSU). Research interests: threshold logic, constructing threshold functions, parameter detection k-valued functions. The number of publications — 3. aburd2011@mail.ru; 4, pr-t Nezavisimosty, Minsk, 220030, Belarus; office phone: +375445737505.

Никонов Владимир Глебович — д-р техн. наук, доцент, член Президиума, Российская академия естественных наук. Область научных интересов: теория запретов k-значных функций, булевы графы, пороговая логика, теория алгоритмов. Число научных публикаций — 200. nikonovu@yandex.ru; Сивцев Вражек пер., 29/16, Москва, 119002; .

Nikonov Vladimir Glebovich — Ph.D., Dr. Sci., associate professor, member of the Presidium of the Russian Academy of natural Sciences. Research interests: bans the theory of k-valued functions, Boolean graphs, threshold logic, the theory of al-Goranov. The number of publications — 200. nikonovu@yandex.ru; 29/16, Sivtsev Vrazhek lane., Moscow, 119002; .

Лапиков Игорь Игоревич — сотрудник, Федеральное государственное унитарное предприятие «Научно-исследовательский институт «КВАНТ». Область научных интересов: методы решения систем линейных неравенств с k-значными неизвестными, метод эллипсоидов, характеризация пороговых функций, теория алгоритмов. Число научных публикаций — 3. landoflord@ya.ru; 4-й Лихачевский пер., 15, Москва, 125438; р.т.: +79114783991.

Lapikov Igor' Igorevich — employee, "RDI "KVANT". Research interests: methods of solving systems of linear inequalities with k-valued unknowns, the method of ellipsoids, the characterization of threshold functions, theory of algorithms. The number of publications — 3. landoflord@ya.ru; 15, 4-th lihachevsky per., Moscow, 125438, Russia; office phone: +79114783991.

РЕФЕРАТ

Бурделев А.В., Никонов В.Г., Лапиков И.И. **Распознавание параметров узла защиты информации, реализованного пороговой k-значной функцией.**

В данной статье рассматриваются аналитический и алгоритмический подходы к распознаванию параметров пороговых k-значных функций, которые могут быть использованы для построения узлов обработки и защиты информации. Основное внимание сосредоточено на проблеме доказательства принадлежности некоторой k-значной функции к классу пороговых. Для аналитического решения этой проблемы предлагается использовать коэффициенты роста и возрастания, на основе которых строится итеративный алгоритм нахождения коэффициентов линейной формы k-значной пороговой функции. На ряду с этим в статье рассматривается алгоритмический подход, основанный на сведении задачи нахождения порогового представления k-значной функции к системе линейных неравенств, для решения которой применяется модифицированный метод эллипсоидов Хачияна. Для рассмотренных подходов приведены результаты экспериментальных исследовании, на основании которых проводится их сравнительный анализ.

SUMMARY

Burdeljov A.V., Nikonov V.G., Lapikov I.I. **Recognizing Parameters of the Information Security Unit Implemented by the Threshold K-Valued Function.**

This article discusses analytical and algorithmic approaches to the recognition of the parameters of the threshold k-valued functions, which can be used for building information processing and security units. The main focus is put on the issue of proving k-valued function belonging to the threshold class. In order to find an analytical solution to this problem it is proposed to use the input coefficients of expansion and increase, based on which an iterative algorithm for finding the coefficients of linear forms of the k-valued threshold function is built. In addition, the article discusses an algorithmic method based on reducing the problem of finding a threshold representation of k-valued functions to the system of linear inequalities, for the solution of which the ellipsoid method, modified by Khachiyan, is applied. The results of experimental research into the analyzed approaches are given. Based on these results the comparative analysis of the approaches is carried out.