

## О ПОРОГОВЫХ И БЛИЗКИХ К НИМ ФУНКЦИЯХ, ОПРЕДЕЛЕННЫХ В ЦЕЛОЧИСЛЕННЫХ ТОЧКАХ ПОЛИТОПА\*)

*Н. Ю. Золотых*

Рассматриваются пороговые и близкие к ним функции, принимающие значения 0 и 1 и определенные на множестве целочисленных точек некоторого фиксированного политопа, заданного системой линейных неравенств. Устанавливаются необходимые и достаточные условия принадлежности функции рассматриваемым классам, приводятся верхние и нижние оценки мощностей таких классов, предлагается алгоритм расшифровки функций из этих классов.

### Введение

Функции  $k$ -значной логики, принимающие значения 0 и 1, можно рассматривать как характеристические функции множеств, определенных на универсе  $\{0, 1, \dots, k-1\}^n$ . В ряде работ ([6, 7] и др.) изучались подклассы таких функций, что подмножество из  $\{0, 1, \dots, k-1\}^n$ , на котором функция равна нулю или (и) единице, можно описать некоторой системой линейных неравенств. Особый интерес представляли пороговые функции. Пороговой функцией  $k$ -значной логики от  $n$  переменных называется отображение гиперкуба  $\{0, 1, \dots, k-1\}^n$  в множество  $\{0, 1\}$ , которое можно задать гиперплоскостью, пересекающей гиперкуб так, что в точках по одну сторону гиперплоскости функция равна нулю, а по другую — единице.

Пусть с каждой функцией  $f$  из некоторого подкласса  $F'$  связан оракул, позволяющий по произвольной точке  $x \in \{0, 1, \dots, k-1\}^n$  определить  $f(x)$ . Под расшифровкой (заранее неизвестной) функции  $f \in F'$  понимается последовательное обращение к оракулу в точках  $x^{(1)}, x^{(2)}, \dots, x^{(t)}$  из  $\{0, 1, \dots, k-1\}^n$ , позволяющее определить  $f(x)$  во всех остальных точках множества  $\{0, 1, \dots, k-1\}^n$ , не прибегая к оракулу. Предполагается, что очередной вопрос к оракулу формируется в зависимости

---

\*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 96-01-00639).

от предыдущих ответов оракула. В [7] при любом фиксированном  $n$  предложен алгоритм расшифровки пороговой функции  $k$ -значной логики, в котором число обращений к оракулу и число используемых операций ограничены некоторыми многочленами от  $\log(k+1)$ .

Поскольку рассматриваемые функции можно интерпретировать как характеристические, естественно стремление расширить их область определения. Пусть множеством определения функции  $f$  является множество  $M$  целочисленных точек некоторого  $n$ -мерного политопа  $P$ , заданного системой линейных неравенств с целочисленными коэффициентами, по абсолютной величине не превосходящими  $\gamma$ . Данная работа посвящена следующим классам линейно отделимых функций, определенных на этом множестве:

- $F_0(M)$  — класс функций, определенных на  $M$ , множество нулей которых можно задать некоторой системой линейных неравенств;
- $F_1(M)$  — класс функций, определенных на  $M$ , множество единиц которых можно задать некоторой системой линейных неравенств;
- класс  $F_0(M) \cap F_1(M)$ ;
- класс пороговых функций  $F_\pi(M)$  — таких функций, для каждой из которых существует гиперплоскость, отделяющая множество нулей от множества единиц.

Класс функций  $k$ -значной логики получается, если  $P$  задается системой неравенств  $0 \leq x_j \leq k-1$  ( $j = 1, \dots, n$ ). Таким образом, работа обобщает результаты из [6] и [7] на случай более широкой области определения: множества целочисленных точек политопа. В § 1 приводятся вспомогательные утверждения. В § 2 даются необходимые и достаточные условия принадлежности функций рассматриваемым классам. Оценки абсолютной величины коэффициентов в неравенствах системы, описывающей множества нулей и единиц функций (т. е. множества, на которых функция равна 0 и 1), и оценки числа крайних точек в выпуклых оболочках этих множеств приводятся в § 3 и 4. В § 5 исследуются мощности рассматриваемых классов. В частности, при  $n \rightarrow \infty$  доказано следующее неравенство:  $\log |F_\pi(M)| < (n^3 \log(\gamma\sqrt{n}))(1 + o(1))$ . В § 6 рассматривается задача расшифровки функций.

Заметим, что расширение области определения на множество целочисленных точек политопа уже рассматривалось в [11] в связи с задачей расшифровки пороговых функций. Здесь рассматривается расшифровка функций из более широкого класса  $F_0(M) \cap F_1(M)$ . При некоторых дополнительных ограничениях и фиксированном  $n$  предлагаемый алгоритм является полиномиальным.

Для любого  $X \subseteq \mathbf{R}^n$  через  $\text{Conv} X$  обозначается выпуклая оболочка множества  $X$ ,  $|M|$  — мощность множества  $M$ ,  $E_k = \{0, 1, \dots, k-1\}$ .

Всюду  $\log$  обозначает логарифм по основанию 2, а  $c_n, c'_n$  — зависящие только от  $n$  константы.

### § 1. Вспомогательные утверждения

Рассмотрим систему  $Ax \leq a_0$ , где  $x \in \mathbb{Z}^n$ ,  $A = (a_{ij}) \in \mathbb{Z}^{m \times n}$ ,  $a_0 = (a_{i0}) \in \mathbb{Z}^m$ . Множество ее решений обозначим через  $M(A, a_0)$ . Пусть  $\alpha = \max\{|a_{ij}|, i = 1, \dots, m; j = 0, 1, \dots, n\} + 1$ .

**Лемма 1** (см., например, [3]). Выпуклая оболочка  $\text{Conv}M(A, a_0)$  является выпуклым многогранным множеством (полиэдром), т. е. может быть описана конечной системой линейных неравенств.

**Лемма 2** (см., например, [3]). Пусть  $Q$  — конечное подмножество множества  $\mathbb{R}^n$ . Тогда число граней максимальной размерности полиэдра  $\text{Conv}Q$  не превосходит  $c_n |Q|^{\lfloor n/2 \rfloor}$ .

Пусть  $N(A, a_0)$  обозначает множество крайних точек в  $\text{Conv}M(A, a_0)$ .

**Лемма 3** [8, с. 53]. Для  $j$ -й координаты любой точки  $x$  из  $N(A, a_0)$  справедливо неравенство  $|x_j| < (n+1)(\alpha\sqrt{n})^n$ ,  $j = 1, \dots, m$ .

**Лемма 4** [8, с. 60]. Справедливо неравенство

$$|N(A, a_0)| \leq c_n m^{\lfloor n/2 \rfloor} \log^{n-1} \alpha.$$

Рассмотрим задачу  $\mathcal{G}_0$  описания множества  $M(A, a_0)$ : по заданным  $A$  и  $a_0$  найти список крайних точек и экстремальных векторов множества  $\text{Conv}M(A, a_0)$ , а также систему линейных неравенств, множество решений которой совпадает с  $\text{Conv}M(A, a_0)$ . В [5] предложен алгоритм, решающий эту задачу. Этот алгоритм опирается на процедуру Ленстры решения в целых числах системы линейных неравенств или доказательства ее несовместности; при любом фиксированном  $n$  алгоритм является полиномиальным. Таким образом, справедлива

**Лемма 5** [5, 8]. Имеется полиномиальный от  $m$  и  $\log \alpha$  алгоритм решения задачи  $\mathcal{G}_0$ .

### § 2. Основные классы линейно отделимых функций

При фиксированных матрице  $C \in \mathbb{Z}^{l \times n}$  и векторе  $c_0 \in \mathbb{Z}^n$  обозначим через  $M$  множество  $M(C, c_0)$ . Пусть  $\gamma = \max\{|c_{ij}|, i = 1, \dots, l, j = 0, \dots, n\} + 1$ . Будем считать, что  $M \neq \emptyset$  и ограничено. Множество всех функций, отображающих  $M$  в  $\{0, 1\}$ , обозначим через  $F(M)$ . Класс

$F(E_2^n)$  состоит из булевых функций, а  $F(E_k^n)$  при  $k \geq 3$  является подклассом класса функций  $k$ -значной логики, принимающих значения 0 и 1. Для  $f \in F(M)$  через  $M_0(f)$  и  $M_1(f)$  обозначим множество нулей и единиц функции  $f$  соответственно, т. е.  $M_\nu(f) = \{x \in M \mid f(x) = \nu\}$  ( $\nu = 0, 1$ ).

Рассмотрим множество  $F_\nu(M)$  ( $\nu = 0, 1$ ) таких функций  $f$  из  $F(M)$ , что множество  $M_\nu(f)$  можно задать системой линейных неравенств  $Ax \leq a_0$ :

$$M_\nu(f) = \{x \in M \mid Ax \leq a_0\}. \quad (1)$$

В этом случае систему  $Ax \leq a_0$  назовем *характеристической*.

**Утверждение 1.** Для того чтобы функция  $f$  из  $F(M)$  принадлежала множеству  $F_\nu(M)$  ( $\nu = 0, 1$ ), необходимо и достаточно, чтобы выполнялось равенство  $\mathbf{Z}^n \cap \text{Conv} M_\nu(f) = M_\nu(f)$ .

**Доказательство.** Необходимость условий очевидна. Для доказательства достаточности заметим, что выпуклая оболочка конечного числа точек описывается системой линейных неравенств [4]. Так как  $\mathbf{Z}^n \cap \text{Conv} M_\nu(f) = M_\nu(f)$ , то условие (1) выполняется.

**Замечание 1.** Элементы матрицы  $A$  и столбца  $a_0$  в описании (1) можно считать целочисленными.

**Замечание 2.** Для любой булевой функции  $f$  справедливо равенство  $\mathbf{Z}^n \cap \text{Conv} M_\nu(f) = M_\nu(f)$  и, следовательно,  $F_0(E_2^n) = F_1(E_2^n) = F(E_2^n)$ . Для функций  $k$ -значной логики при  $k \geq 3$  аналогичные равенства не выполняются.

Обозначим через  $m_\nu(f)$  наименьшее число неравенств в системе  $Ax \leq a_0$ , при котором возможно задание функции  $f \in F_\nu(M)$  в виде (1), а через  $N_\nu(f)$  — множество крайних точек политопа  $\text{Conv}(M_\nu(f))$ . Если  $f \in F_\nu(M)$  и  $m_\nu(f) = 1$  при  $\nu = 0$  или  $\nu = 1$ , то функция  $f$  называется *пороговой*. Пусть для такой  $f$  неравенство

$$\sum_{j=1}^n a_j x_j \leq a_0, \quad (2)$$

которое называется *пороговым*, описывает множество  $M_\nu(f)$ , т. е.

$$M_\nu(f) = \left\{ x \in M \mid \sum_{j=1}^n a_j x_j \leq a_0 \right\}. \quad (3)$$

Поскольку по замечанию 1 можно считать, что  $a_j \in \mathbf{Z}$  ( $j = 0, 1, \dots, n$ ), то

$$M_{1-\nu}(f) = \left\{ x \in M \mid \sum_{j=1}^n a_j x_j \geq a_0 + 1 \right\}, \quad (4)$$

т. е.  $f \in F_{1-\nu}(M)$  и  $m_{1-\nu}(f) = 1$ . Обозначим через  $F_\pi(M)$  множество всех заданных на  $M$  пороговых функций.

**Утверждение 2.** Условие

$$\text{Conv}(M_0(f)) \cap \text{Conv}(M_1(f)) = \emptyset \quad (5)$$

является необходимым и достаточным для того, чтобы функция  $f$  из класса  $F(M)$  была пороговой.

**Доказательство.** Необходимость. Пусть  $f \in F_\pi(M)$ . Тогда для  $M_\nu(f)$  ( $\nu = 0, 1$ ) существуют описания в виде (3) и (4). Отсюда следует соотношение (5). Достаточность вытекает из теоремы о разделяющей гиперплоскости (см., например, [4]).

### § 3. Величина коэффициентов системы, задающей линейно отделимые функции

С каждой функцией  $f \in F_\pi(M)$  в  $(n+2)$ -мерном пространстве связан конус  $K(f)$  разделяющих функционалов  $(a_0, a_1, \dots, a_n, a_{n+1})$ , описываемый следующей системой линейных неравенств (ср. [6]):

$$\begin{cases} \sum_{j=1}^n a_j x_j \leq a_0 & \text{для всех } x = (x_1, \dots, x_n) \in M_0(f); \\ \sum_{j=1}^n a_j x_j \geq a_0 + a_{n+1} & \text{для всех } x = (x_1, \dots, x_n) \in M_1(f); \\ a_{n+1} \geq 0. \end{cases} \quad (6)$$

Любое решение  $(a_0, \dots, a_{n+1})$  этой системы при  $a_{n+1} > 0$  определяет некоторое пороговое неравенство (2) для функции  $f$ . Верно и обратное: коэффициенты  $(a_0, \dots, a_{n+1})$  любого порогового неравенства функции  $f \in F(M)$  удовлетворяют системе (6) при некотором положительном  $a_{n+1}$ . Очевидно, что (6) эквивалентна системе

$$\begin{cases} \sum_{j=1}^n a_j x_j \leq a_0 & \text{для всех } x = (x_1, \dots, x_n) \in N_0(f); \\ \sum_{j=1}^n a_j x_j \geq a_0 + a_{n+1} & \text{для всех } x = (x_1, \dots, x_n) \in N_1(f); \\ a_{n+1} \geq 0. \end{cases} \quad (7)$$

Из теории линейных неравенств [4] следует, что в  $K(f)$  существует такая система векторов  $b^{(1)}, \dots, b^{(s)}$  (порождающая система), что любой  $b$  из  $K(f)$  является их линейной комбинацией с неотрицательными

коэффициентами. Кроме того,  $b^{(i)}$  ( $i = 1, \dots, s$ ) может быть выбран так, что его  $j$ -я координата  $b_j^{(i)}$  с точностью до знака совпадает с некоторым определителем порядка не более  $n + 1$ , составленного из коэффициентов системы (6). Используя неравенство Адамара и оценку из леммы 2, получаем  $|b_j^i| \leq (n + 1)^{(n+1)/2} ((n + 1) \gamma^n n^{n/2})^{n+1}$ . Следовательно,

$$|b_j^i| \leq ((n + 1)^{3/2} n^{n/2} \gamma^n)^{n+1}. \quad (8)$$

Отсюда вытекает

**Следствие 1.** Для любой функции  $f$  из  $F_\pi(M)$  существует пороговое неравенство (2) с целочисленными коэффициентами, модули которых не превосходят правой части из (8).

**Следствие 2.** Для любого  $\nu = 0, 1$  и любой функции  $f$  из  $F_\nu(M)$  существует характеристическая система  $Ax \leq a_0$  с целочисленными коэффициентами, модули которых не превосходят правой части из (8).

**Доказательство.** Рассмотрим пороговую функцию  $f_i$  такую, что  $M_0(f_i)$  описывается  $i$ -м неравенством системы  $Ax \leq a_0$ , и воспользуемся следствием 2.

Для пороговых функций  $k$ -значной логики (т. е. при  $M = E_k^n$ ) оценка запишется в виде:  $|b_j^i| \leq ((n + 1)^{3/2} n^{n/2} (k - 1)^n)^{n+1}$ . В [7] для этого частного случая найдена более точная оценка:  $|b_j^i| \leq (n + 1)^{1+n/2} 2^{-n-1} (k - 1)^{n-1}$ . При  $k = 2$  она превращается в известную оценку величины коэффициентов порогового неравенства функций из  $F_\pi(E_2^n)$

$$|a_j| \leq (n + 1)^{1+n/2} 2^{-n-1}. \quad (9)$$

Оценку (9) дополняет нижняя оценка величины коэффициентов порогового неравенства из [10]. Для  $n = 2^q$  ( $q \geq 2, q \in \mathbb{N}$ ) в [10] указана функция  $F_n$ , коэффициенты порогового неравенства которой нельзя сделать меньше величины

$$\frac{1}{2n} e^{-4n^\beta} 2^{(n \ln n)/2 - n},$$

где  $\beta = \log(3/2)$ . Очевидно, эта оценка является также нижней оценкой величины коэффициентов порогового неравенства для функций из  $F_\pi(E_k^n)$ .

#### § 4. Число крайних точек в $\text{Conv}\{M_\nu(f)\}$ ( $\nu = 0, 1$ )

Для  $\nu = 0, 1$  рассмотрим систему линейных неравенств, полученную из системы  $Cx \leq c_0$  добавлением к ней неравенств  $Ax \leq a_0$  из (1). Так как модули коэффициентов новой системы ограничены величиной из правой части неравенства (8), из леммы 4 и следствия 2 получаем

**Утверждение 3.** Если  $f \in F_\nu(M)$  ( $\nu = 0, 1$ ), то  $|N_\nu(f)| \leq c_n(l + m_\nu(f))^{[n/2]} \log^{n-1} \gamma$  ( $\nu = 0, 1$ ).

Таким образом, для каждой функции  $f$  из  $F_\nu(M)$  ( $\nu = 0, 1$ ) при любом фиксированном  $n$  число крайних точек  $|N_\nu(f)|$  ограничено сверху полиномом от  $l$ ,  $m_\nu(f)$  и  $\gamma$ . Для класса пороговых функций получаем

**Утверждение 4.** Если  $f \in F_\pi(M)$ , то  $|N_\nu(f)| \leq C_n l^{[n/2]} \log^{n-1} \gamma$  ( $\nu = 0, 1$ ).

Рассмотрим задачу  $\mathcal{G}_1$  нахождения множеств  $N_\nu(f)$  и всех неравенств — граней множества  $\text{Conv} M_\nu(f)$  для функции  $f \in F_\nu(M)$  ( $\nu = 0, 1$ ) по заданной целочисленной системе  $Cx \leq c_0$ , описывающей  $M$ , и системе  $Ax \leq a_0$ , описывающей  $M_\nu(f)$ . Из утверждения 4 и леммы 5 вытекает

**Утверждение 5.** Пусть функция  $f$  из  $F_\nu(M)$  ( $\nu = 0, 1$ ) задана характеристической системой  $Ax \leq a_0$ , где  $A \in \mathbb{Z}^{m_\nu(f) \times n}$  и  $a_0 \in \mathbb{Z}^n$ , коэффициенты которой удовлетворяют неравенству (8). Тогда при фиксированном  $n$  существует полиномиальный от  $m_\nu(f)$ ,  $l$  и  $\log \gamma$  алгоритм решения задачи  $\mathcal{G}_1$ .

### § 5. Мощности классов линейно отделимых функций

Нахождение числа функций из рассматриваемых классов является сложной задачей. Для величины  $|F_\pi(E_2^n)|$  известна лишь полученная Ю. А. Зуевым [1] (см. также [2]) асимптотика для ее логарифма. Для функций  $k$ -значной логики и функций, определенных на множестве  $M$ , задача усложняется.

Рассмотрим класс  $F_\nu(M, r)$  таких функций  $f$  из  $F_\nu(M)$ , что  $m_\nu(f) = r$  ( $\nu = 0, 1$ ).

**Теорема 1.** При любых  $\gamma \geq 1$ ,  $r \geq 1$  и  $n \rightarrow \infty$  справедливо неравенство  $\log |F_\nu(M, r)| < (rn^3 \log(\gamma\sqrt{n}))(1 + o(1))$ .

**Доказательство.** Из следствия 2 получаем, что системами  $r$  неравенств с целочисленными коэффициентами, ограниченными по абсолютной величине числом из правой части неравенства (8), описываются все возможные функции из класса  $F_\nu(M, r)$  ( $\nu = 0, 1$ ). Поэтому

$$|F_\nu(M, r)| \leq (2((n+1)^{3/2} n^{n/2} \gamma^n)^{n+1} + 1)^{r(n+1)}$$

и, следовательно,

$$\log |F_\nu(M, r)| < r \left( \frac{3}{2} n^2 \log n + n^3 \log(\gamma\sqrt{n}) \right) (1 + o(1)).$$

Теорема 1 доказана.

Заметив, что  $F_0(M, 1) = F_1(M, 1) = F_\pi(M)$ , получаем

**Следствие 3.** При любом  $\gamma \geq 1$  и  $n \rightarrow \infty$  справедливо неравенство  $\log |F_\pi(M)| < (n^3 \log(\gamma\sqrt{n}))(1 + o(1))$ .

В случае функций  $k$ -значной логики в [8] найдены более точные оценки:  $\log |F_\nu(E_k^n, r)| < (rn^2 \log(k\sqrt{n}))(1 + o(1))$  ( $\nu = 0, 1$ ),  $\log |F_\pi(E_k^n)| < n^2 \log k(1 + o(1))$ .

**Лемма 6** [8]. Если  $k \geq 2$ ,  $n \geq 2$ , то

$$|F_\pi(E_k^n)| > 2k^{1+n(n-1)/2}. \quad (10)$$

**Доказательство.** Обобщим рассуждения работы [9] для  $k = 2$  на случай произвольного  $k \geq 2$ . Каждой функции  $f$  из  $F_\pi(E_k^n)$ , задаваемой неравенством (2), поставим в соответствие все функции из  $F_\pi(E_k^{n+1})$ , задаваемые пороговым неравенством

$$\sum_{j=1}^n a_j x_j + a x_{n+1} \leq a_0, \quad (11)$$

где  $a$  пробегает множество  $\mathbf{R}$ . Пусть в неравенстве (11) коэффициенты выбраны так, что ни при каком  $a$  пороговая гиперплоскость не пересекает более одной точки из  $E_k^{n+1} \cap \{x = (x_1, \dots, x_n, 1)\}$ . В этом случае в подкубе  $E_k^{n+1} \cap \{x = (x_1, \dots, x_n, 1)\}$  возникает  $k^n + 1$  функций. Таким образом, при варьировании параметра  $a$  из каждой функции  $f \in F_\pi(E_k^n)$  получаем не менее  $k^n + 1$  функций из  $F_\pi(E_k^{n+1})$ . Поэтому  $|F_\pi(E_k^{n+1})| \geq (k^n + 1)|F_\pi(E_k^n)|$ , откуда при  $k \geq 2$  и  $n \geq 2$  следует неравенство

$$|F_\pi(E_k^n)| \geq |F_\pi(E_k^1)| \prod_{i=1}^{n-1} k^i = |F_\pi(E_k^1)| \cdot k^{n(n-1)/2}.$$

Легко видеть, что  $|F_\pi(E_k^1)| = 2k$ , а значит,  $|F_\pi(E_k^n)| \geq 2k^{1+n(n-1)/2}$ . Лемма 6 доказана.

Пусть  $\mathcal{P}(n, \gamma)$  — множество политопов  $P \subseteq \mathbf{R}^n$ , которые можно задать системой линейных неравенств с целочисленными коэффициентами, модули которых меньше  $\gamma$ , и

$$\varphi_\pi(n, \gamma) = \max_{P \in \mathcal{P}(n, \gamma)} |F_\pi(\mathbf{Z}^n \cap P)|.$$

Из леммы 6 следует

**Теорема 2.** При любых  $\gamma \geq 2$  и  $n \geq 2$

$$\log \varphi_\pi(n, \gamma) > \frac{n(n-1)}{2} \log \gamma.$$

Пользуясь следствием 3 и теоремой 2, получаем



**Следствие 4.** При любом  $\gamma \geq 2$  и  $n \rightarrow \infty$

$$\frac{n(n-1)}{2} \log \gamma < \log \phi_\pi(n, \gamma) < (n^3 \log(\gamma \sqrt{n}))(1 + o(1)).$$

При  $k = 2$  в [1] получено асимптотическое равенство  $\log |F_\pi(E_2^n)| \sim n^2$ , из которого следует  $\log |F_\pi(E_k^n)| > n^2(1 - o(1))$ . Автору неизвестно, как использовать аппарат из [1, 2] для получения более высоких нижних оценок для  $|F_\pi(E_k^n)|$ .

### § 6. Расшифровка функций из класса $F_0(M) \cap F_1(M)$

Под *расшифровкой* функции  $f$  из класса  $F' \subseteq F(M)$  понимается последовательное обращение к оракулу в точках  $x^{(1)}, x^{(2)}, \dots, x^{(t)}$  из  $M$ , позволяющее по значениям в этих точках определить  $f(x)$  во всех остальных точках множества  $M$ , не прибегая к оракулу. *Сложностью*  $\tau(\mathcal{A})$  алгоритма расшифровки  $\mathcal{A}$  функций из класса  $F' \subseteq F(M)$  называется минимальное число обращений к оракулу, достаточное для расшифровки алгоритмом  $\mathcal{A}$  любой функции из класса  $F'$ . *Трудоёмкостью* алгоритма  $\mathcal{A}$  назовем число арифметических операций, необходимых в худшем случае. Как и выше, будем предполагать, что политоп  $P$  задан целочисленной системой линейных неравенств, а  $M = \mathbf{Z}^n \cap P$ .

В работе [11] предложен алгоритм  $\mathcal{A}_1$  расшифровки функции из класса  $F_\pi(M)$  полиномиальной (от  $l$  и  $\log \gamma$ ) трудоёмкости, причем  $\tau(\mathcal{A}_1) \leq c_n l^{\lfloor n/2 \rfloor} \log^n \gamma$ .

Здесь предлагается алгоритм  $\mathcal{A}_0$  расшифровки функций из более широкого класса  $F_0(M) \cap F_1(M)$ . Для функции  $f$  алгоритм  $\mathcal{A}_0$  находит  $N_\nu(f)$  для некоторого  $\nu = 0, 1$ . Дальнейшее вычисление  $f(x)$  сводится затем к определению принадлежности  $x$  выпуклой оболочке множества  $N_\nu(f)$ .

**Лемма 7.** Существует алгоритм  $\mathcal{A}_2$ , который для любой функции  $f \in F_{1-\nu}(M)$  ( $\nu = 0, 1$ ) и для любого  $a = (a_1, \dots, a_n) \in \mathbf{Z}^n$  находит такую точку  $y = (y_1, \dots, y_n) \in M_\nu(f)$ , что

$$\sum_{j=1}^n a_j y_j = \max \left\{ \sum_{j=1}^n a_j x_j; (x_1, \dots, x_n) \in M_\nu(f) \right\},$$

или устанавливает, что  $M_\nu(f) = \emptyset$ . При любом фиксированном  $n$  алгоритм имеет полиномиальную от  $l$  и  $\log \alpha$  трудоёмкость и совершает не более  $c'_n l^{\lfloor n/2 \rfloor} \log^n \alpha$  обращений к оракулу, где  $\alpha = \max\{\gamma, |a_j|, j = 1, \dots, n\}$ .

Доказательство. По лемме 3 для любой точки  $x = (x_1, \dots, x_n)$  из  $M$  выполняется неравенство  $|\sum_{j=1}^n a_j x_j| \leq \sum_{j=1}^n (n+1)(\gamma\sqrt{n})^n |a_j|$ . Таким образом,

$$\left| \sum_{j=1}^n a_j x_j \right| \leq \xi, \quad (12)$$

где  $\xi = n^{1+n/2}(n+1)\alpha^{n+1}$ . Следовательно,

$$\max_{x \in M_\nu(f)} \left\{ \sum_{j=1}^n a_j x_j \right\} - \min_{x \in M_\nu(f)} \left\{ \sum_{j=1}^n a_j x_j \right\} \leq 2n^{1+n/2}(n+1)\alpha^{n+1}.$$

Из леммы 5 получаем, что для любого целого  $a_0$  такого, что  $|a_0| \leq \xi$ , с полиномиальной (от  $l$  и  $\log \alpha$ ) трудоемкостью можно построить множество  $N(a, a_0, P)$ . Здесь и далее  $N(a, a_0, P)$  обозначает множество крайних точек политопа  $\text{Conv}(\{x = (x_1, \dots, x_n) \mid \sum_{j=1}^n a_j x_j \geq a_0\} \cap P \cap \mathbb{Z}^n)$ . По лемме 4 имеем

$$|N(a, a_0, P)| \leq c_n l^{\lfloor n/2 \rfloor} \log^{n-1} \alpha. \quad (13)$$

Обращаясь к оракулу не более чем  $|N(a, a_0, P)|$  раз, можно найти точку  $x \in M_\nu(f) \cap N(a, a_0, P)$  или убедиться, что таких точек не существует. Так как  $f \in F_{1-\nu}(M)$ , то из равенства  $M_\nu(f) \cap N(a, a_0, P) = \emptyset$  (что эквивалентно выполнению равенства  $f(x) = 1 - \nu$  для любой точки  $x \in N(a, a_0, P)$ ) следует, что  $f(x) = 1 - \nu$  для любой точки  $x = (x_1, \dots, x_n)$  из  $M$  такой, что  $\sum_{j=1}^n a_j x_j \geq a_0$ , т. е. если  $x = (x_1, \dots, x_n) \in M_\nu(f)$ , то  $\sum_{j=1}^n a_j x_j \leq a_0 - 1$ .

Опишем теперь алгоритм  $\mathcal{A}_2$ . Выбрав в качестве  $a$  и  $a_0$  коэффициенты какого-либо неравенства из системы, описывающей политоп  $P$ , и обратившись к оракулу в точках из  $N(a, a_0, P)$ , либо выясним, что  $M_\nu(f) = \emptyset$ , либо найдем некоторую точку из  $M_\nu(f)$ . В последнем случае выполним также следующие действия.

**Алгоритм  $\mathcal{A}_2$ .**

**Шаг 1.** Полагается  $u := -\xi$ ;  $v := \xi$ .

**Шаг 2.** Полагается  $w := \lfloor (u + v)/2 \rfloor$ .

**Шаг 3.** Находится  $N(a, w, P)$ .

**Шаг 4.** Если  $N(a, w, P) \cap M_\nu(f) = \emptyset$ , то полагается  $v := w$ . В противном случае с помощью оракула находится какая-нибудь точка  $y = (y_1, \dots, y_n) \in N(a, w, P) \cap M_\nu(f)$  и полагается  $u := w$ .

**Шаг 5.** Если  $u = v - 1$ , то стоп, иначе переход на шаг 2.

Шаги 1–5 являются дихотомией по отрезку  $[-\xi, \xi]$ , находящей такую точку  $y = (y_1, \dots, y_n)$ , что  $\sum_{j=1}^n a_j y_j = w = \max \left\{ \sum_{j=1}^n a_j x_j; x \in M_\nu(f) \right\}$ .

Очевидно, что число итераций этой процедуры не превосходит величины  $[1 + \log 2\xi]$ . Учитывая трудоемкость построения множества  $N(a, a_0, P)$ , получаем, что трудоемкость алгоритма  $\mathcal{A}_2$  полиномиальна от  $l$  и  $\log \alpha$ .

Из оценок (12) и (13) следует, что число обращений к оракулу в данной процедуре не превосходит величины  $c_n l^{[n/2]} [1 + \log 2\xi] \log^{n-1} \alpha \leq c'_n l^{[n/2]} \log^n \alpha$ . Лемма 7 доказана.

**Лемма 8.** Если  $f \in F_0(M) \cap F_1(M)$ , то для любого  $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$  точка  $p$ , выдаваемая алгоритмом  $\mathcal{A}_2$ , является крайней точкой множества  $\text{Conv} M_\nu(f)$ .

**Доказательство.** Покажем, что при  $f \in F_0(M) \cap F_1(M)$  и  $M_\nu(f) \neq \emptyset$  алгоритм  $\mathcal{A}_2$ , описанный в доказательстве леммы 7, выдает точку  $p = (p_1, \dots, p_n)$  из множества  $N_\nu(f)$ . Предположим, что  $p \notin N_\nu(f)$ . Тогда найдутся такие  $p^{(i)} = (p_1^{(i)}, \dots, p_n^{(i)}) \neq p$  из  $M_\nu(f)$  и такие числа  $\alpha_i > 0$  ( $i = 1, \dots, s$ ), что  $\sum_{i=1}^s \alpha_i = 1$  и

$$p = \sum_{i=1}^s \alpha_i p^{(i)}. \quad (14)$$

Поэтому

$$\sum_{j=1}^n a_j p_j = \sum_{i=1}^s \alpha_i \sum_{j=1}^n a_j p_j^{(i)} = w, \quad (15)$$

где  $w$  — найденный максимум. Так как  $\alpha_i > 0$ ,  $\sum_{i=1}^s \alpha_i = 1$ , то из (15)

следует, что либо найдется такое  $i' = 1, \dots, s$ , что  $\sum_{j=1}^n a_j p_j^{(i')} > w$ , либо

для каждого  $i = 1, \dots, s$  выполняется равенство  $\sum_{j=1}^n a_j p_j^{(i)} = w$ . В первом

из этих случаев  $p$  не является точкой максимума, а во втором — ввиду (14)  $p \notin N(a, w, P)$ . Лемма 8 доказана.

Рассмотрим множество  $F(M, h)$  таких функций  $f$  из  $F_0(M) \cap F_1(M)$ , что  $\min \{m_0(f), m_1(f)\} \leq h$ .

**Теорема 3.** Существует алгоритм  $\mathcal{A}_0$  расшифровки функций из класса  $F_0(M) \cap F_1(M)$ , который при любом фиксированном  $n$  расшифровывает функции из класса  $F(M, h)$  с полиномиальной (от  $h$ ,  $l$  и  $\log \gamma$ ) трудоемкостью и имеет сложность

$$\tau(\mathcal{A}_1) \leq c_n (l + h)^{[n/2]^2} l^{[n/2]} \log^{(n-1)[n/2] + n} \gamma.$$

**ДОКАЗАТЕЛЬСТВО.** Прежде чем перейти к пошаговому описанию алгоритма  $\mathcal{A}_0$ , дадим некоторые комментарии. Алгоритм  $\mathcal{A}_0$  с помощью вспомогательной процедуры  $\mathcal{A}_2$  последовательно находит крайние точки множеств  $\text{Conv}M_\nu(f)$  ( $\nu = 0, 1$ ), запоминая их в  $S_\nu \subseteq N_\nu(f)$ . Неравенства системы, описывающей  $P_\nu(f)$ , накапливаются в  $H_\nu$ .  $H'_\nu$  содержит неравенства из описания  $\text{Conv}S_\nu$ , не вошедшие в  $H_\nu$ .

Неравенство из системы  $H$  назовем *эквивалентным* неравенству  $h'$  относительно  $H$ , если после замены первого вторым множество решений системы  $H$  не изменилось. Известно (см. [3]), что для нахождения общего решения целочисленной системы линейных неравенств при любом фиксированном числе переменных  $n$  существуют полиномиальные алгоритмы. На их основе легко построить алгоритмы, проверяющие эквивалентность пар неравенств.

### Алгоритм $\mathcal{A}_0$ .

**Шаг 0.** Пусть  $H_\nu$  ( $\nu = 0, 1$ ) — пустая система линейных неравенств. Алгоритм определяет  $f(x)$  для всех вершин множества  $\text{Conv}M$ . Обозначим через  $S_\nu$  ( $\nu = 0, 1$ ) множество тех из них, для которых  $f(x) = \nu$ . Если при  $\nu = 0$  или при  $\nu = 1$  множество  $S_\nu$  пусто, то расшифровка закончена, так как в этом случае  $M_\nu(f) = \emptyset$ .

**Шаг 1.** Для каждого  $\nu = 0, 1$  находится неприводимая система линейных неравенств, описывающая  $\text{Conv}S_\nu$ ; из этой системы удаляются те неравенства, для каждого из которых в  $H_\nu$  существует ему эквивалентное (относительно исходной системы) неравенство. Полученную систему обозначим через  $H'_\nu$ .

**Шаг 2.** Для каждого  $\nu = 0, 1$  алгоритм выполняет последовательность шагов 2.1–2.4 и возвращается на шаг 1.

**Шаг 2.1.** Если система  $H'_\nu$  пуста, то  $N_\nu(f) = S_\nu$  и расшифровка закончена.

**Шаг 2.2.** В  $H'_\nu$  выбирается произвольное неравенство  $\sum_{j=1}^n a_j x_j \leq a_0$  и исключается из  $H'_\nu$ .

**Шаг 2.3.** С помощью алгоритма  $\mathcal{A}_2$  находится точка  $p = (p_1, \dots, p_n) \in N_\nu(f)$ , максимизирующая  $\sum_{j=1}^n a_j x_j$  на множестве  $M_\nu(f)$ .

**Шаг 2.4.** Если  $\sum_{j=1}^n a_j p_j \leq a_0$ , то алгоритм добавляет к  $H_\nu$  неравенство  $\sum_{j=1}^n a_j x_j \leq a_0$  и переходит на шаг 2.1, в противном случае алгоритм присоединяет  $p$  к  $S_\nu$ .

Для доказательства корректности алгоритма  $\mathcal{A}_0$  заметим, что на шаге 0 при любом  $\nu = 0, 1$  справедливо включение  $S_\nu \subseteq N_\nu(f)$  и если

$S_\nu = \emptyset$ , то по утверждению 2  $M_\nu(f) = \emptyset$ . Легко видеть, что алгоритм завершит свою работу, когда для некоторого  $\nu = 0, 1$  все точки  $x \in M_\nu(f)$  будут удовлетворять системе  $H_\nu$ , т. е. при  $S_\nu = N_\nu(f)$ .

Оценим сложность и трудоемкость алгоритма  $\mathcal{A}_0$ . По лемме 5 все вершины множества  $\text{Conv}M$  на шаге 0 можно построить при фиксированном  $n$  за полиномиальное от  $l$  и  $\log \gamma$  время. Лемма 4 гарантирует, что число обращений к оракулу на этом шаге не больше  $c_n l^{\lfloor n/2 \rfloor} \log^{n-1} \gamma$ . Для нахождения на шаге 1 системы, описывающей  $\text{Conv}S_\nu$ , достаточно решить  $\binom{|S_\nu|}{n}$  систем  $n$  линейных уравнений от  $n+1$  неизвестных. Как и в следствии 1, из неравенства Адамара следует, что при фиксированном  $n$  абсолютные величины найденных таким образом коэффициентов ограничены сверху некоторым полиномом от  $\gamma$ . Учитывая, что количество систем, которые нужно решить, полиномиально от  $|S_\nu|$ , для процедуры шага 1 при фиксированном  $n$  получаем алгоритм, полиномиальный от  $|S_\nu|$ ,  $\log \gamma$  и числа неравенств в  $H_\nu$ . На каждой итерации шага 2 для каждого  $\nu = 0, 1$  к  $S_\nu$  присоединяется лишь одна точка. Следовательно, ввиду того, что  $S_\nu \subseteq N_\nu(f)$ , получаем  $|S_\nu| \leq |N_{\nu'}(f)|$ , где  $\nu'$  определяется из равенства  $m_{\nu'}(f) = h$ . Учитывая оценку из утверждения 3, получаем

$$|S_\nu| \leq c_n(l+h)^{\lfloor n/2 \rfloor} \log^{n-1} \gamma. \quad (16)$$

Для дальнейшего доказательства сделаем несколько очевидных замечаний. Во-первых, на шаге 2.4 к  $H_\nu$  добавляются только неравенства, соответствующие опорным к  $\text{Conv}M_\nu(f)$  и  $\text{Conv}S_\nu$  гиперплоскостям. Во-вторых, каждое такое неравенство либо описывает некоторую фасету (грань максимальной размерности) политопа  $\text{Conv}S_\nu$ , либо является неявным равенством (см., например, [4, § 8.1, 8.4]). Из леммы 2 получаем следующую оценку на число  $|H_\nu|$  неравенств в системе  $H_\nu$ :  $|H_\nu| \leq c_n |N_\nu(f)|^{\lfloor n/2 \rfloor}$ . Так как при каждом обращении к алгоритму  $\mathcal{A}_2$  происходит добавление нового элемента либо к  $H_\nu$ , либо к  $S_\nu$ , из оценки (14) получаем, что количество этих обращений, а также общее число итераций шага 2 не превосходит величины  $c_n |S_\nu|^{\lfloor n/2 \rfloor} \leq c'_n(l+h)^{\lfloor n/2 \rfloor^2} \log^{\lfloor n/2 \rfloor(n-1)} \gamma$ . Принимая во внимание количество обращений к оракулу в алгоритме  $\mathcal{A}_2$  и на шаге 0 алгоритма  $\mathcal{A}_0$ , получаем

$$\tau(\mathcal{A}_0) \leq c_n(l+h)^{\lfloor n/2 \rfloor^2} l^{\lfloor n/2 \rfloor} \log^{(n-1)\lfloor n/2 \rfloor + n} \gamma.$$

При фиксированном  $n$  величины  $|S_\nu|$ ,  $|H_\nu|$  ограничены полиномами от переменных  $h$ ,  $l$ ,  $\log \gamma$ . Следовательно, при фиксированном  $n$  алгоритм  $\mathcal{A}_0$  полиномиален. Теорема 3 доказана.

Так как  $F_\pi(M) \subseteq F_0(M) \cap F_1(M)$ , то алгоритм  $\mathcal{A}_0$  применим и к классу  $F_\pi(M)$ , однако верхняя оценка его сложности хуже, чем у алгоритма  $\mathcal{A}_1$ . Если известно, что  $f \in F_0(M) \cap F_1(M)$ , то алгоритм  $\mathcal{A}_0$  позволяет найти множества  $N_\nu(f)$  ( $\nu = 0, 1$ ), а затем построить систему линейных неравенств, эквивалентную (6), и ее порождающую систему  $b^{(1)}, \dots, b^{(s)}$ . Если существуют  $b^{(i)}$  с положительной последней координатой, то  $f \in F_\pi(M)$ , в противном случае  $f \notin F_\pi(M)$ . Так как трудоемкость вычисления каждого  $b^{(i)}$  полиномиальна, то справедлива

**Теорема 4.** При любом фиксированном  $n$  для функции  $f \in F_0(M) \cap F_1(M)$  существует полиномиальный от  $l$ ,  $m_0(f)$ ,  $m_1(f)$ ,  $\log \gamma$  алгоритм распознавания пороговости и построения конуса  $K(f)$ .

Автор благодарит В. Н. Шевченко за полезные обсуждения и постоянное внимание к работе и рецензента за ценные замечания и новые для автора библиографические сведения.

## ЛИТЕРАТУРА

1. Зуев Ю. А. Асимптотика логарифма числа пороговых функций алгебры логики // Докл. АН СССР. 1989. Т. 306, № 3. С. 528–530.
2. Ирматов А. А. О числе пороговых функций // Дискрет. математика. 1993. Т. 5, вып. 3. С. 40–43.
3. Схрейвер А. Теория линейного и целочисленного программирования: В 2 т. М.: Мир, 1991.
4. Черников С. Н. Линейные неравенства. М.: Наука, 1968.
5. Шевченко В. Н. Алгебраический подход в целочисленном программировании // Кибернетика. 1984. № 4. С. 36–41.
6. Шевченко В. Н. О некоторых функциях многозначной логики, связанных с целочисленным программированием // Методы дискретного анализа в теории графов и схем: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1985. Вып. 42. С. 99–108.
7. Шевченко В. Н. О расшифровке пороговых функции многозначной логики // Комбинаторно-алгебраические методы в прикладной математике. Горький: Горьк. гос. ун-т, 1987. С. 155–163.
8. Шевченко В. Н. Качественные вопросы целочисленного программирования. М.: Физматлит, 1995.
9. Яджима С., Ибараки Т. Нижняя оценка числа пороговых функций // Кибернетический сб. М.: Мир, 1969. Вып. 6. Н. С. С. 72–81.

10. **Håstad J.** On the size of weights for threshold gates // SIAM J. Discrete Math. 1994. V. 7, N 3. P. 484–492.
11. **Shevchenko V. N., Zolotikh N. Y.** Decoding of threshold functions defined on integer points of a polytope // Pattern Recognition and Image Analysis. 1997. V. 7, N 2. P. 235–240.

Адрес автора:

Нижегородский  
государственный университет,  
пр. Гагарина, 23,  
603600 Нижний Новгород,  
Россия

Статья поступила

19 июня 1997 г.,  
переработанный вариант —  
20 февраля 1998 г.