ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 519.6

РАСШИФРОВКА ПОРОГОВОЙ ФУНКЦИИ, ЗАДАННОЙ РАСШИРЕННЫМ ОРАКУЛОМ

Н.Ю. Золотых

Нижегородский госуниверситет им. Н.И. Лобачевского

nikolai.zolotykh@gmail.com

Поступила в редакцию 24.02.2012

Предлагается алгоритм расшифровки пороговой функции k-значной логики n переменных, заданной с помощью оракула, позволяющего по произвольной точке x из $\mathbb{R}^n$ определить, удовлетворяет ли x пороговому неравенству, или нет. При фиксированном n алгоритм имеет полиномиальную от $\log k$ трудоемкость и использует асимптотически не более $\frac{n^4}{2}\log(n+1)+2n^3\log_2 k$ обращений к оракулу.

Ключевые слова: пороговая функция, расшифровка.

Введение

Пороговой функцией k-значной логики, зависящей от n переменных, называется такое отображение f множества $E_k^n=\{0,1,\ldots,k-1\}^n$ в $\{0,1\}$, при котором существует гиперплоскость, отделяющая множество $M_0(f)=\{x\in E_k^n : f(x)=0\}$ «нулей» функции f от множества $M_1(f)=\{x\in E_k^n : f(x)=1\}$ ее «единиц», т.е. найдутся числа $a_0, a_1,\ldots, a_n$, такие, что

$$M_0(f)=\left\{x\in E_k^n : \sum_{j=1}^n a_j x_j \le a_0\right\}.$$

Очевидно, что *пороговое неравенство*

$$\sum_{j=1}^n a_j x_j \le a_0, \qquad (1)$$

определяющее пороговую функцию f, может быть задано неоднозначно.

Множество всех пороговых функций, заданных на E_k^n, обозначим $\Pi(n,k)$. Всюду предполагается, что $n\ge 1$, $k\ge 2$.

В ряде работ, например, [1–5], рассматривается задача *расшифровки* пороговой функции. Предполагается, что функция f задана *оракулом*, позволяющим по произвольной точке $x\in E_k^n$ определить значение $f(x)$. Под расшифровкой заранее не известной пороговой функции f понимается процедура восстановления коэффициентов $a_0, a_1,\ldots, a_n$ любого возможного порогового неравенства функции f с помощью обращений к ее оракулу. Существуют [1, 2] алгоритмы расшифровки произвольной функции $f\in\Pi(n,k)$, при фиксированном n требующие полиномиального от $\log_2 k$ времени и использующие не более $c_n\log_2^n k$ обращений к оракулу. С другой стороны, доказано [3, 4], что никакой алгоритм расшифровки пороговой функции при $n\ge 2$ не может использовать (в худшем случае) менее, чем $d_n\log_2^{n-2} k$ обращений к оракулу. Здесь c_n и d_n – некоторые величины, зависящие только от n. Лучшие известные значения для c_n и d_n приведены в [5].

В настоящей работе мы исследуем задачу расшифровки пороговой функции, заданной более информативным – «расширенным» – оракулом, который в отличие от «обычного» оракула принимает на вход произвольные точки из $\mathbb{R}^n$, а не только из E_k^n. *Расширенный оракул* связан с конкретным пороговым неравенством (1) функции f. По заданной точке $x\in\mathbb{R}^n$ он возвращает 0, если неравенство (1) выполнено, и 1 в противном случае (если ясно, о каком пороговом неравенстве идет речь, будем писать тогда $f(x)=0$ и $f(x)=1$ соответственно). Под *расшифровкой* пороговой функции f, заданной с помощью расширенного оракула, будем понимать процедуру восстановления коэффициентов ее любого возможного порогового неравенства с помощью обращений к этому оракулу.

Мы предлагаем алгоритм расшифровки пороговой функции, заданной расширенным оракулом. При фиксированном n алгоритм имеет полиномиальную от $\log_2 k$ трудоемкость и использует асимптотически не более $\frac{n^4}{2}\log_2(n+1) + 2n^3\log_2 k$ обращений к оракулу.

1. Вспомогательные результаты

Лемма 1 [6, 7]. Для любой функции $f \in \Pi(n,k)$ существует пороговое неравенство (1), в котором коэффициенты $a_0, a_1,\ldots, a_n$ – целые, причем

$$|a_0| \le \frac{(n+1)^{\frac{n}{2}+1}}{2^n}(k-1)^n,$$

$$|a_j| \le \frac{(n+1)^{\frac{n}{2}+1}}{2^{n+1}}(k-1)^{n-1} \quad (j=1,2,\ldots,n).$$

Обозначим

$$\Xi = \frac{(n+1)^{\frac{n}{2}+1}}{2^n}(k-1)^n. \qquad (2)$$

Пусть $\Pi_+(n,k)$ – множество тех функций из $\Pi(n,k)$, для каждой из которых $f(0) = 0$. Из леммы 1 легко получается

Лемма 2. Для любой функции $f \in \Pi_+(n,k)$ найдется пороговое неравенство (1), в котором коэффициенты $a_0, a_1,\ldots, a_n$ – целые, причем $a_0 > 0$ и

$a_j > 0$, если $f(-\Xi e_j) < f(\Xi e_j)$;
$a_j = 0$, если $f(-\Xi e_j) = f(\Xi e_j)$;
$a_j < 0$, если $f(-\Xi e_j) > f(\Xi e_j)$.

Обозначим e_j вектор в $\mathbb{R}^n$, все компоненты которого равны 0, кроме j-й, равной 1.

Лемма 3. Пусть $y^{(j)} = \beta_j e_j \in \mathbb{R}^n$, $z^{(j)} = \gamma_j e_j \in \mathbb{R}^n$ ($j = 1,2,\ldots,n$), причем $\gamma_j > 0$, $\beta_j > 0$, $0 \le \gamma_j - \beta_j \le \varepsilon$, где

$$\varepsilon = \frac{2^{n-1}}{(k-1)^{n-1}(n+1)^{\frac{n+1}{2}}}. \qquad (3)$$

Тогда множество $D = E_k^n \cap \operatorname{conv}\{y^{(1)}, y^{(2)}, \ldots, y^{(n)}, z^{(1)}, z^{(2)}, \ldots, z^{(n)}\}$ либо пусто, либо найдется гиперплоскость, на которой располагаются все точки из D.

Доказательство. Если аффинная размерность множества D меньше n, то утверждение леммы очевидно. В противном случае в D найдется аффинно независимая система точек $x^{(1)}, x^{(2)},\ldots, x^{(n)}$. Коэффициенты гиперплоскости $\sum_{j=1}^{n} a_j x_j = a_0$, проходящей через эти точки, определяются единственным образом с точностью до постоянного множителя. Их можно выбрать так, что a_j с точностью до знака равно минору, полученному вычеркиванием j-го столбца из матрицы, составленной из компонент точек $x^{(1)}, x^{(2)},\ldots, x^{(n)}$ и дополненной столбцом из единиц. Пользуясь оценкой определителя с неотрицательными элементами (см., например, [8]), получаем

$$a_0 \le \frac{(k-1)^n (n+1)^{\frac{n+1}{2}}}{2^n},$$

$$a_j \le \frac{(k-1)^{n-1}(n+1)^{\frac{n+1}{2}}}{2^n} = \frac{1}{2\varepsilon} \quad (j=1,2,\ldots,n).$$

Так как a_j – целые по построению, то область R, заданная неравенствами $a_0 - 1 \le \sum_{j=1}^{n} a_j x_j \le a_0 + 1$, не содержит других точек из E_k^n, кроме точек, лежащих на гиперплоскости $\sum_{j=1}^{n} a_j x_j = a_0$.

Покажем, что $D \subset R$. Для всякого $j = 1,2,\ldots,n$ рассмотрим точки $v^{(j)} = \frac{a_0}{a_j}\cdot e_j$, $u^{(j)} = \frac{a_0 - 1}{a_j}\cdot e_j$ и $w^{(j)} = \frac{a_0 + 1}{a_j}\cdot e_j$. Точка $v^{(j)}$, очевидно, принадлежит гиперплоскости $\sum_{j=1}^{n} a_j x_j = a_0$ и отрезку $[y^{(j)}, z^{(j)}]$. Точки $y^{(j)}$, $z^{(j)}$, $v^{(j)}$ принадлежат отрезку $[u^{(j)}, w^{(j)}]$. Так как длина отрезка $[y^{(j)}, z^{(j)}]$ не превосходит ε, а длина отрезка $[u^{(j)}, w^{(j)}]$ равна $2/a_j \ge 4\varepsilon > 2\varepsilon$, то делаем вывод, что $y^{(j)}$ и $z^{(j)}$ принадлежат R для каждого $j = 1,2,\ldots,n$, откуда $D \subset R$, что завершает доказательство леммы.

2. Алгоритм

Опишем алгоритм $\mathfrak{A}$ расшифровки функции $f \in \Pi(n,k)$, заданной расширенным оракулом.

Шаг 1. Обращаемся к оракулу в точке 0. Если $f(0) = 0$, то $f \in \Pi_+(n,k)$. Далее будем считать, что это условие выполнено, так как в противном случае функцию f можно заменить на $1 - f \in \Pi_+(n,k)$.

Шаг 2. С помощью $2n$ обращений к оракулу найдем значения функции f в точках $\pm\Xi e_j$ ($j = 1,2,\ldots,n$), где Ξ определяется формулой (2). Если $f(\Xi e_j) = f(-\Xi e_j)$ для некоторого j, то ввиду леммы 2 найдется пороговое неравенство функции f, в котором $a_j = 0$, т.е. переменная x_j является несущественной и задача расшифровки сводится к задаче меньшей размерности. Для всякого j, такого, что $f(-\Xi e_j) > f(\Xi e_j)$, выполним

замену переменных $x_j \mapsto k-1-x_j$, тем самым сводя задачу к расшифровке пороговой функции, в которой для любого ее порогового неравенства выполнено

$$a_j > 0 \quad (j = 0,1,\ldots,n), \tag{4}$$

т.е. такой монотонной пороговой функции, в которой все переменные существенны. Далее будем предполагать, что свойство (4) выполнено.

Шаг 3. Для каждого j = 1,2,…,n с помощью дихотомии на отрезке [0, Ξe_j] находим такие $y^{(j)}$, $z^{(j)}$, для которых $|y^{(j)} - z^{(j)}| \le \varepsilon$, где ε определяется формулой (3). Согласно лемме 3 в результате получим многогранную область P, такую, что $D = P \cap E_k^n$ либо пусто, либо найдется гиперплоскость, на которой располагаются все точки из D. Определить, какой случай имеет место, и (если $D \ne \varnothing$) построить эту гиперплоскость можно с помощью полиномиального при фиксированном n алгоритма построения вершин выпуклой оболочки целочисленных решений заданной системы линейных неравенств (см. [7, теорема 5.7, с. 111]).

Если $D = \varnothing$, то процедура расшифровки закончена. Действительно, если K_0, K_1 – множества точек, в которых в ходе работы алгоритма происходило обращение к оракулу, и в которых значение f равно 0 и 1 соответственно, то легко видеть, что $M_0(f) = K_0 \cap E_k^n$, $M_1(f) = K_1 \cap E_k^n$.

Если $D \ne \varnothing$, то задача сводится к расшифровке функции из класса $\Pi(n-1,k')$, где $k' \le k\sqrt{n}$.

Теорема. При любом фиксированном n алгоритм $\mathfrak{A}$ является полиномиальным от log$k$ и использует не более

$$\frac{(6n^2+n+11)(n+1)n}{12}\log(n+1) + n^2(2n-1)\log_2 k$$

обращений к расширенному оракулу функции f.

Доказательство. На шагах 1 и 2 алгоритма $\mathfrak{A}$ происходит 2n + 1 обращений к оракулу. Процедура дихотомии на шаге 3 для каждого j = = 1,2,…,n использует

$$\log_2 \frac{\Xi}{\varepsilon} = \log_2 \frac{(n+1)^{n+\frac{3}{2}}}{2^{2n-1}}(k-1)^{2n-1}$$

обращений к оракулу. Обозначая через τ(n,k) максимально возможное число обращений к оракулу при расшифровке функции из класса Π(n,k), получаем

$$\tau(n,k) \le 2n+1+$$
$$+n\left(\left(n+\frac{3}{2}\right)\log_2(n+1) - 2n + 2 + (2n-1)\log_2(k-1)\right) +$$
$$+\tau\left(n-1, k\sqrt{n}\right),$$

откуда

$$\tau(n,k) \le \sum_{m=1}^{n}\left(m\left(m+\frac{3}{2}\right)\log_2(m+1) - m(2m-1)\right) +$$
$$+n(2n-1)\left(n\log_2 k + \sum_{m=1}^{n}\frac{m}{2}\log_2 n\right).$$

После преобразований имеем

$$\tau(n,k) \le \frac{(6n^2+n+11)(n+1)n}{12}\log(n+1) -$$
$$-\frac{(4n-1)(n+1)n}{6} + n^2(2n-1)\log_2 k,$$

откуда получаем требуемое. Так как все вспомогательные процедуры на каждом шаге алгоритма можно выполнить за время, полиномиальное от $\log_2 k$ (при фиксированном n), то общее время работы алгоритма при фиксированном n также ограничено некоторым полиномом от $\log_2 k$.

Работа выполнена в рамках федеральной целевой программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007-2013 годы», госконтракт 11.519.11.4015.

Список литературы

1. Золотых Н.Ю., Шевченко В.Н. Расшифровка пороговых функций k-значной логики // Дискретный анализ и исследование операций. 1995. Т. 2. № 3. С. 18–23.

2. Hegedus T. Generalized teaching dimensions and the query complexity of learning // Proc. 8th Ann. ACM Conf. on Computational Learning Theory (COLT'95). New York: ACM Press, 1995. P. 108–117.

3. Шевченко В.Н., Золотых Н.Ю. О сложности расшифровки пороговых функций k-значной логики // Доклады Академии наук. 1998. Т. 362. № 5. С. 606–608.

4. Золотых Н.Ю., Шевченко В.Н. О нижней оценке сложности расшифровки пороговых функций k-значной логики // Журнал вычислительной математики и математической физики. 1999. Т. 39. № 2. С. 346–352.

5. Золотых Н.Ю. Оценки мощности минимального разрешающего множества пороговой функции многозначной логики // Математические вопросы кибернетики. Вып. 17. М.: Физматлит, 2008. С. 159–168.

6. Шевченко В.Н. О некоторых функциях многозначной логики, связанных с целочисленным программированием // Методы дискретного анализа в теории графов и схем. Вып. 42. Новосибирск: Ин-т матем. СО АН СССР, 1985. С. 99–108.

7. Шевченко В.Н. Качественные вопросы целочисленного программирования. М.: Физматлит, 1995.

8. Мишина А.П., Проскуряков И.В. Высшая алгебра. Линейная алгебра, многочлены, общая алгебра. М.: Наука, 1965.

DECIPHERING A THRESHOLD FUNCTION DEFINED BY AN EXTENDED ORACLE

N.Yu. Zolotykh

An algorithm is proposed for deciphering a threshold function of k-valued logic of k variables defined by an oracle allowing determination for any x from $\mathbb{R}^n$ whether or not the threshold inequality is satisfied. For fixed n the algorithm has a polynomial in $\log k$ complexity and uses no more than $\frac{n^4}{2}\log(n+1) + 2n^3 \log_2 k$ queries to the oracle.

Keywords: threshold function, deciphering.