

РАСШИФРОВКА ПОРОГОВЫХ ФУНКЦИЙ k -ЗНАЧНОЙ ЛОГИКИ*)

Н. Ю. Золотых, В. Н. Шевченко

Рассматривается задача расшифровки пороговых функций k -значной логики от n переменных. Предлагается алгоритм расшифровки полиномиальной сложности, который при фиксированном n использует не более $O(\log^n(k+1))$ обращений к оракулу.

Введение

Рассмотрим следующую игру двух лиц. На игровом поле $B(2, k)$, состоящем из всех точек $(x, y) \in Z^2$ таких, что $0 \leq x \leq k-1$, $0 \leq y \leq k-1$, первый игрок выбирает две различные точки и находит уравнение $ax + by = c$ прямой, проходящей через них. Второй игрок должен найти уравнение этой прямой, выбирая точки $(x_i, y_i) \in B(2, k)$ и задавая первому игроку вопрос, верно ли, что $ax_i + by_i \leq c$. С точки зрения второго игрока, естественно найти стратегию, гарантирующую получение ответа с небольшим числом вопросов и приемлемым временем вычисления координат (x_i, y_i) . Обобщая эту ситуацию, введем следующие обозначения и понятия [1, 2].

Пусть k и n — натуральные числа, $B(n, k)$ — множество целочисленных векторов $\mathbf{x} = (x_1, x_2, \dots, x_n)$ таких, что $0 \leq x_j \leq k-1$ ($j = 1, 2, \dots, n$); $f(\mathbf{x})$ — функция, отображающая $B(n, k)$ в множество $\{0, 1\}$; $M_0(f)$ и $M_1(f)$ — множества векторов $\mathbf{x} = (x_1, x_2, \dots, x_n)$ таких, что $f(\mathbf{x})$ равна нулю или единице соответственно, т. е. $M_0(f) = \{\mathbf{x} \in B(n, k) \mid f(\mathbf{x}) = 0\}$, $M_1(f) = \{\mathbf{x} \in B(n, k) \mid f(\mathbf{x}) = 1\}$; $N_i(f)$ — множество крайних точек выпуклой оболочки множества $M_i(f)$ ($i = 0, 1$).

Функция $f(\mathbf{x})$ называется *пороговой*, если существуют действительные числа a_i ($i = 0, 1, \dots, n$) такие, что

$$M_0(f) = \{\mathbf{x} \in B(n, k) \mid \sum_{i=1}^n a_i x_i \leq a_0\}. \quad (1)$$

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 94-01-00491).

Множество всех пороговых функций, заданных на $B(n, k)$, обозначим через $F(n, k)$.

Пусть с функцией $f \in F(n, k)$ связан оракул, позволяющий по любой точке $x \in B(n, k)$ вычислить $f(x)$. Такой оракул назовем *М-оракулом*. Под *М-расшифровкой* функции $f \in F(n, k)$ понимается процедура нахождения с помощью *М-оракула* таких чисел a_0, a_1, \dots, a_n , при которых выполняется равенство (1).

Алгоритм *А* *М-расшифровки* пороговой функции назовем *полиномиальным*, если для любой функции $f \in F(n, k)$ число $\tau(A)$ обращений к оракулу и число $\rho(A)$ необходимых при этом вычислений ограничены сверху некоторыми полиномами от n и $\log(k+1)$. (Здесь и всюду в дальнейшем \log обозначает логарифм по основанию 2.) В [2] доказано несуществование полиномиального алгоритма *М-расшифровки* пороговой функции. При фиксированной размерности n полиномиальный алгоритм назовем *квазиполиномиальным*.

В [1] было замечено, что для задания пороговой функции f достаточно знать множество $N_0(f)$ или $N_1(f)$, и показано, что

$$|N_i(f)| \leq (2 \log(k+1))^n \quad (i = 0, 1).$$

В [3] был предложен квазиполиномиальный алгоритм для построения выпуклой оболочки множества M целочисленных решений системы линейных неравенств, опирающийся на алгоритм Ленстры [4] нахождения точки $x \in M$ и оценку из [5] для числа крайних точек и граней выпуклой оболочки множества M . Эти результаты существенно использовались в полученном в [2] квазиполиномиальном алгоритме A_1 расшифровки пороговой функции. Позднее [6, 7] верхняя оценка $\tau(A_1)$ понижается вследствие уточнения [3, 8, 9] верхних оценок для $|N|$; в [7] она имеет вид

$$\tau(A_1) = O((\log(k+1))^{n+\lfloor n/2 \rfloor (n-1)}).$$

Заметим, что дальнейшее понижение показателя степени на этом пути, по-видимому, невозможно, поскольку полученная в [10] оценка для числа крайних точек не улучшаема по порядку [11, 12].

Мы предлагаем квазиполиномиальный алгоритм A_2 расшифровки функции $f \in F(n, k)$ такой, что $\tau(A_2) = O(\log^n(k+1))$.

Для построения алгоритма используются результаты работы [13], в которой с пороговой функцией связан более информативный оракул. Этот оракул назовем *Е-оракулом*. Он определяется следующим образом. *Е-оракул* функции $f \in F(n, k)$ по любому набору целых чисел a_0, a_1, \dots, a_n выдает ответ «да», если $M_0(f)$ удовлетворяет равенству (1), в противном случае оракул выдает ответ «нет» и точку $z = (z_1, z_2,$

$\dots, z_n)$ из $B(n, k)$ такую, что либо $\sum_{i=1}^n a_i z_i > a_0$ и $f(z) = 0$ (положительный контрпример), либо $\sum_{i=1}^n a_i z_i \leq a_0$ и $f(z) = 1$ (отрицательный контрпример). Под *E-расшифровкой* функции f из класса $F(n, k)$ понимается последовательность обращений к *E*-оракулу, позволяющая получить ответ «да».

При построении алгоритма A_2 в § 2 покажем, что вместо одного обращения к *E*-оракулу достаточно $O(\log^{n-1}(k+1))$ раз обратиться к *M*-оракулу.

§ 1. Вспомогательные результаты

Сначала переформулируем следующий результат работы [10].

Лемма 1. Пусть P — полиэдр, заданный системой m линейных неравенств с целочисленными коэффициентами, по абсолютной величине не превосходящими α , $M(P)$ — пересечение P с целочисленной решеткой, $N(P)$ — множество крайних точек выпуклой оболочки множества $M(P)$. Тогда при любых фиксированных m и n справедливо соотношение $|N(P)| = O(\log \alpha^{n-1})$.

Лемма 2. Пусть *E*-оракулу предъявляются коэффициенты a_0, a_1, \dots, a_n с длиной двоичной записи, ограниченной сверху некоторым полиномом от $\log(k+1)$. Тогда любое такое обращение к *E*-оракулу с полиномиальной от $\log(k+1)$ трудоемкостью можно свести к $O(\log^{n-1}(k+1))$ вопросам *M*-оракулу (n фиксировано).

Доказательство. Во-первых, при помощи алгоритма из [3] построим множество $N(a_0, a_1, \dots, a_n)$ вершин выпуклой оболочки множества

$$\{x \in B(n, k) \mid \sum_{i=1}^n a_i x_i \leq a_0\}.$$

Далее с помощью *M*-оракула, последовательно проверяя значение f в каждой из этих точек, найдем точку $z \in N(a_0, a_1, \dots, a_n)$ такую, что $f(z) = 1$, либо установим, что такой точки нет. Очевидно, что в первом случае z будет являться отрицательным контрпримером. Во втором случае построим множество $N'(a_0, a_1, \dots, a_n)$ вершин выпуклой оболочки множества

$$\{x \in B(n, k) \mid \sum_{i=1}^n a_i x_i > a_0\}$$

и будем обращаться к *M*-оракулу в каждой точке из $N'(a_0, a_1, \dots, a_n)$ до тех пор, пока не найдем точку $z' \in N'(a_0, a_1, \dots, a_n)$ такую, что $f(z') = 0$,

либо установим, что такой точки нет. В первом случае z' , очевидно, является положительным контрпримером, а во втором, как следует из [1],

$$M_0(f) = \{x \in B(n, k) \mid \sum_{i=1}^n a_i x_i \leq a_0\},$$

т. е. функция f расшифрована.

Таким образом, мы свели одно обращение к E -оракулу к серии обращений к M -оракулу. Оценим число таких обращений и число необходимых арифметических операций. В [1] показано, что при фиксированном n для любой $f \in F(n, k)$ существуют такие целые $b_j (j = 0, 1, \dots, n)$, что $|b_j|$ ограничен некоторым полиномом от k и

$$M_0(f) = \{x \in B(n, k) \mid \sum_{i=1}^n b_i x_i \leq b_0\}.$$

Отсюда и из леммы 1 следует, что при любом фиксированном n справедливо соотношение

$$|N(a_0, a_1, \dots, a_n)| = |N(b_0, b_1, \dots, b_n)| = O(\log^{n-1}(k+1));$$

аналогично можно показать, что $|N'(a_0, a_1, \dots, a_n)| = O(\log^{n-1}(k+1))$. Поэтому число обращений к M -оракулу, необходимых для сведения одного обращения к E -оракулу, не превосходит $O(\log^{n-1}(k+1))$.

Оценим сверху число выполненных при этом арифметических операций. Для нахождения точек множества $N(b_0, b_1, \dots, b_n)$ мы воспользовались алгоритмом, предложенным в [3].

Трудоемкость этого алгоритма при фиксированном n ограничена некоторым полиномом от $\log(\alpha + 1)$, где $\alpha = \max\{k, a_0, a_1, \dots, a_n\}$. Так как при фиксированном n длина двоичной записи коэффициентов a_0, a_1, \dots, a_n ограничена сверху полиномом от $\log(k+1)$, то число операций, необходимых для сведения одного обращения к E -оракулу к серии обращений к M -оракулу, ограничено сверху некоторым полиномом от $\log(k+1)$. Лемма 2 доказана.

§ 2. Основные результаты

Дадим некоторые пояснения к предложенному в [13] алгоритму A_3 E -расшифровки пороговой функции.

Алгоритм A_3 использует алгоритм нахождения точки в выпуклом теле $W \subseteq \mathbb{R}^n$, заданном *оракулом отделения* (см., например, [14]). Оракул отделения для W по точке $b \in \mathbb{R}^n$ выдает ответ «да», если $b \in W$; в противном случае оракул выдает ответ «нет» и коэффициенты какой-нибудь гиперплоскости, отделяющей b от W .

Не нарушая общности (см. [13]), можно считать, что для функции f из $F(n, k)$ в выражении (1) коэффициент $a_0 = 1$. Следовательно, в пространстве \mathbb{R}^n каждой пороговой функции f соответствует выпуклое тело $W(f) = \{u \in \mathbb{R}^n \mid M_0(f) = \{x \mid (u, x) \leq 1\}\}$.

Таким образом, задача E -расшифровки пороговой функции может быть сформулирована как задача нахождения какой-либо точки из $W(f)$.

В [13] указан способ построения оракула отделения для $W(f)$ на основе E -оракула для функции f . В качестве алгоритма нахождения точки в выпуклом теле можно использовать алгоритм эллипсоидов [14, 15].

Сформулируем результат из [13] в виде теоремы.

Теорема 1 [13]. Существует алгоритм A_3 E -расшифровки пороговой функции, причем при любом фиксированном n $\tau(A_3) = O(\log k)$, а $\rho(A_3)$ и длина двоичной записи каждого коэффициента a_0, a_1, \dots, a_n при всех обращениях к E -оракулу ограничены сверху некоторыми полиномами от $\log(k+1)$.

Из теоремы 1 и леммы 2 вытекает следующее утверждение.

Теорема 2. При любом фиксированном n существует полиномиальный алгоритм M -расшифровки пороговой функции k -значной логики от n переменных, который использует не более $C_n \log^n(k+1)$ вопросов о значении функции $f(x)$ в точке x , где C_n — некоторая константа, зависящая только от n .

ЛИТЕРАТУРА

1. 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.
2. Шевченко В. Н. О расшифровке пороговой функции многозначной логики // Комбинаторно-алгебраические методы и их применения. Горький: Горьк. ун-т, 1987. С. 155–163.
3. Шевченко В. Н. Алгебраический подход в целочисленном программировании // Кибернетика. 1984. № 4. С. 36–41.
4. Lenstra H. W., Jr. Integer programming with a fixed number of variables // Math. Oper. Res. 1983. V. 8, N 4. P. 538–548.
5. Шевченко В. Н. Выпуклые многогранные конусы, системы сравнений и правильные отсечения в целочисленном программировании // Комбинаторно-алгебраические методы в прикладной математике. Горький: Горьк. ун-т, 1979. С. 109–119.

6. Шевченко В. Н., Веселов С. И. Расшифровка функций многозначной логики//Теория и программная реализация методов дискретной оптимизации. Киев, 1989. С. 30–34.
7. Hegedus T. Geometrical concept learning and convex polytopes//Proc. of the 7th annu. conf. on computational learning theory. New Brunswick, NJ: ACM Press, 1994.
8. Шевченко В. Н. Верхние оценки числа крайних точек в целочисленном программировании// Математические вопросы кибернетики. М.: Наука, 1992. Вып. 4. С. 65–72.
9. Чирков А. Ю., Шевченко В. Н. О числе вершин выпуклой оболочки пересечения полиэдра с целочисленной решеткой. Нижний Новгород: Нижегород. ун-т, 1993. 12 с. Деп. в ВИНТИ 29.07.93, № 2165-B93.
10. Cook W., Hartmann M., Kannan R., McDiarmid C. On integer points in polihedra//Combinatorica. 1992. V. 12, N 1. P. 27–37.
11. Веселов С. И. Нижняя оценка среднего числа неприводимых и крайних точек в двух задачах дискретного программирования//Горький: Горьк. ун-т, 1984. 8 с. Деп. в ВИНТИ 03.06.84, № 619-B84.
12. Чирков А. Ю. Нижняя оценка числа вершин выпуклой оболочки пересечения полиэдра с целочисленной решеткой//Нижний Новгород: Нижегород. ун-т, 1994. 6 с. Деп. в ВИНТИ 03.06.94, № 1361-B94.
13. Maas W., Turan G. How fast can a threshold gate learn?//PIG-Report Ser. Rep. 321. Graz Univ. of Technology, 1991.
14. Схрейвер А. Теория линейного и целочисленного программирования. М.: Мир, 1991.
15. Хачиян Л. Г. Полиномиальный алгоритм в линейном программировании//Докл. АН СССР. 1979. Т. 244, № 5. С. 1093–1096.

Адрес авторов:

Россия,
603600 Нижний Новгород,
пр. Гагарина, 23,
Нижегородский
государственный
университет
им. Н. И. Лобачевского

Статья поступила

23 ноября 1994 г.