УДК 512.55 DOI 10.17223/2226308X/10/63

О ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ МЕТОДА ЭЛЛИПСОИДОВ ДЛЯ РАСПОЗНАВАНИЯ ПОРОГОВЫХ ФУНКЦИЙ

И. И. Лапиков

Для распознавания принадлежности произвольной булевой функции к классу пороговых предлагается использовать модификацию метода эллипсоидов, предложенную Л. Г. Хачияном. Полиномиальная сложность данного алгоритма позволяет сделать вывод о полиномиальной сложности задачи распознавания принадлежности произвольной булевой функции к классу пороговых.

Ключевые слова: *пороговые функции, метод эллипсоидов, алгоритм Хачияна.*

Предложенный в 1979 году Л. Г. Хачияном алгоритм решения систем линейных неравенств с целочисленными коэффициентами и действительными неизвестными

$$a_{i1}x_1 + \ldots + a_{in}x_n \leqslant b_i, \quad i = 1, \ldots, m, \tag{1}$$

позволил классифицировать сложность данной задачи как полиномиальную [1]. Сложность алгоритма характеризуется значением максимального количества итераций

$$w = 6n^2L,$$

где $L = \left[\sum\limits_{i,j=1}^{m,n} \log_2(|a_{i,j}| + 1) + \sum\limits_{i=1}^{m} \log_2(|b_i| + 1) + \log_2 mn\right] + 1$ — длина входа алгоритма, т. е. количество битов, необходимых для записи системы (1) в двоичном виде.

Алгоритм основан на построении последовательности эллипсоидов убывающего объёма. Важно подчеркнуть, что после выполнения указанного числа итераций алгоритм либо обнаруживает искомое решение, либо позволяет заключить, что система (1) несовместна. Метод эллипсоидов допускает множественное применение для решения различных прикладных математических задач.

Рассмотрим важную проблему пороговой логики — задачу распознавания принадлежности произвольной булевой функции к классу пороговых [2 – 4].

Определение 1. Булева функция $\tau(x_1, \ldots, x_n)$ называется *пороговой*, если для неё существует линейное неравенство с действительными коэффициентами

$$a_ix_i + \ldots + a_nx_n > b, \tag{2}$$

которое выполняется на тех и только тех наборах $(x_1, \ldots, x_n)$, для которых $\tau(x_1, \ldots, x_n) = 1$. Коэффициенты a_i называются *весами*, а b — *порогом*.

Задача проверки, является ли произвольная булева функция $f(x_1, \ldots, x_n)$ пороговой, несмотря на простоту постановки, является сложной. Для её решения предложены итеративные алгоритмы [5, 6]. Стоит отметить, что данная задача может быть сведена к анализу и решению систем линейных неравенств вида (1). Действительно, произвольная булева функция $f(x_1, \ldots, x_n)$ может быть задана таблично. В предположении, что f — пороговая, подстановка в неравенство (2) наборов $(\varepsilon_1^{(i)}, \ldots, \varepsilon_1^{(i)})$, на которых функция равна 1, приведёт к выполнению неравенства, а наборов $(\delta_1^{(i)}, \ldots, \delta_1^{(i)})$, на которых функция равна 0, — к его невыполнению. Таким образом, будет построена система

$$\begin{cases} a_i\varepsilon_1^{(i)} + \ldots + a_n\varepsilon_n^{(i)} \geqslant b, \\ a_i\delta_1^{(i)} + \ldots + a_n\delta_n^{(i)} < b, \end{cases}$$

которая по существу является системой вида (1). Таким образом, применение метода эллипсоидов позволяет решить задачу характеризации пороговой функции с полиномиальной и заведомо известной сложностью.

Отмечая высокую принципиальную значимость этого результата, следует, тем не менее, признать, что для пороговых функций, как показывают эксперименты, итеративные алгоритмы, как правило, выигрывают у метода эллипсоидов. Однако ни один из известных на сегодняшний день итеративных алгоритмов не позволяет дать отрицательного ответа, то есть что заданная произвольная булева функция не является пороговой, в то время как метод эллипсоидов эту задачу решает. Практические примеры применения алгоритма Хачияна и его модификаций выявили ещё одну особенность этого метода — рост модуля коэффициентов $a_j^{(i)}$ в ходе работы алгоритма. С целью получения дискретных значений текущие действительные выражения для $a_j^{(i)}$ требуют корректировки, для которой необходимо построение самостоятельной процедуры. Корректировка может включать процедуры деноминации текущих значений и их округления.

Определение 2. Под *деноминацией* будем понимать снижение значения a_i за счёт деления на 10^d при подходящим образом выбранном d. Коэффициент d будем называть *порядком деноминации*.

Рассмотрим процедуры распознавания принадлежности булевой фукции к классу пороговых и деноминации на примере. Пусть булева функция f от трёх переменных задана таблично:

x_1	x_2	x_3	$f(x_1,x_2,x_3)$	x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	1	1	0	0	1
0	0	1	0	1	0	1	1
0	1	0	0	1	1	0	0
0	1	1	0	1	1	1	0

По описанной выше методике сформируем систему линейных неравенств:

$$\begin{cases} b_0 \leqslant 0, \\ a_3 - b_0 \leqslant -1, \\ a_2 - b_0 \leqslant -1, \\ a_2 + a_3 - b_0 \leqslant -1, \\ -a_1 + b_0 \leqslant 0, \\ -a_1 - a_3 + b_0 \leqslant 0, \\ a_1 + a_2 - b_0 \leqslant -1, \\ a_1 + a_2 + a_3 - b_0 \leqslant -1. \end{cases} \tag{3}$$

Решим систему (3) модифицированным методом эллипсоидов [7]. Алгоритм находит решение системы за 6 итераций и получает вектор решений $X = (a_1, a_2, a_3, b_0) = (411789793{,}477,\ -445309873{,}255,\ -207254306{,}819,\ -5919482{,}343)$. Проведём процедуру деноминации полученного решения с порядком $d = 6$ и округление. В результате получим вектор $X = (a_1, a_2, a_3, b_0) = (411,\ -445,\ -207,\ -6)$ и пороговое представление булевой функции f:

$$f(\varepsilon_1, \varepsilon_2, \varepsilon_3) = 0 \Leftrightarrow L(\varepsilon_1, \varepsilon_2, \varepsilon_3) < -6.$$

Здесь $L(\varepsilon_1, \varepsilon_2, \varepsilon_3) = 411\varepsilon_1 - 445\varepsilon_2 - 207\varepsilon_3$.

В данном примере порядок деноминации равен только 6, но практические эксперименты показывают значительный рост порядка деноминации при увеличении количества аргументов функции. Это обусловливает необходимость проверки принадлежности полученного в результате деноминации и округления решения к многограннику решений рассматриваемой системы неравенств. Поскольку в примере найдено решение системы (3), принадлежащее многограннику её решений, можно сделать вывод, что функция f принадлежит к классу пороговых; если бы метод эллипсоидов показал несовместность системы (3), то можно было бы утверждать, что функция не является пороговой.

Таким образом, сделаем вывод о возможности применения метода эллипсоидов для распознавания пороговых булевых функций. Детальное изучение процесса его работы и сравнительный анализ с итеративными алгоритмами, в том числе в k-значной области, представляет актуальное направление для дальнейших исследований.

ЛИТЕРАТУРА

1. *Хачиян Л. Г.* Полиномиальные алгоритмы в линейном программировании // ЖВМиМФ. 1980. Вып. 20. № 1. С. 51–68.
2. *Зуев А. Ю.* Пороговые функции и пороговые представления булевых функций // Математические вопросы кибернетики. 1994. № 5. С. 5–61.
3. *Никонов В. Г.* Пороговые представления булевых функций // Обозрение прикл. и промышл. математики. 1994. Вып. 1. № 3. С. 458–545.
4. *Кудрявцев Л. Г.* Теория тестового распознавания // Дискретная математика. 2006. Вып. 18. № 3. С. 3–34.
5. *Бурделев А. В., Никонов В. Г., Лапиков И. И.* Распознавание параметров узла защиты информации, реализованного пороговой k-значной функцией // Труды СПИИРАН. 2016. Вып. 46. С. 108–127 .
6. *Дертоузос П.* Пороговая логика. М.: Мир, 1967. 344 с.
7. *Лапиков И. И., Никонов В. Г.* Адаптивный алгоритм решения систем неравенств с k-значными неизвестными // Труды Военно-космической академии им. А. Ф. Можайского. 2016. Вып. 1. С. 88–94.

УДК 512.55 DOI 10.17223/2226308X/10/64

ПРИМЕНЕНИЕ ПОРОГОВЫХ ПРИБЛИЖЕНИЙ ДЛЯ РЕШЕНИЯ СИСТЕМ НЕЛИНЕЙНЫХ УРАВНЕНИЙ В МЕТОДЕ РАЗДЕЛЯЮЩИХ ПЛОСКОСТЕЙ

В. Г. Никонов, А. Н. Шурупов

В методе разделяющих плоскостей предлагается перейти от системы линейных неравенств, эквивалентной нелинейному булеву уравнению, к системе линейных неравенств, являющейся следствием исходного уравнения. Вводится понятие импликативного k-приближения в пороговом базисе, которое характеризуется, с одной стороны, числом k линейных неравенств, а с другой стороны, дефицитом — мерой близости импликативного приближения к исходной системе неравенств. Предельный случай — 1-приближение, как и остальные, не является однозначным. Отказ от свойства импликативности позволяет ввести понятие статистического порогового приближения для булевой функции. Введённые понятия могут быть использованы для сокращения числа линейных неравенств в системе, порождённой исходным нелинейным уравнением, с сохранением возможности её решения.