УДК 512.55 DOI 10.17223/2226308X/8/18

НЕКОТОРЫЕ СТРУКТУРНЫЕ СВОЙСТВА КВАДРАТИЧНЫХ БУЛЕВЫХ ПОРОГОВЫХ ФУНКЦИЙ

А. Н. Шурупов

На основе бинарного отношения частичного порядка, заданного на множестве квадратичных форм с булевыми переменными, предлагается способ описания классов квадратичных булевых пороговых функций (к.б.п.ф.), одновременно допускающих (или не допускающих) нетривиальную декомпозицию. Указаны представители классов, функциональная разделимость которых означает выполнение этого свойства и для всех функций из класса. В частных случаях исследована существенная зависимость к.б.п.ф. от своих переменных.

Ключевые слова: *квадратичная булева пороговая функция, декомпозиция, существенная переменная.*

Полиномиальные булевы пороговые функции определяются следующим образом [1]:

$$f(x_1,\dots,x_n)=0 \Leftrightarrow g(x_1,\dots,x_n)\leqslant 0, \tag{1}$$

где g — действительный полином. Если $\deg g=2$, то говорят о к.б.п.ф. В последнем случае неравенство из (1) может быть преобразовано в эквивалентное $q(x_1,\dots,x_n)\leqslant t$, где q — квадратичная форма, а t — свободный член многочлена g, взятый с противоположным знаком и называемый порогом.

Пусть $A_w=\{\{w(x):x\in\{0,1\}^n\}\}$ — мультимножество значений квадратичной формы $w(x)$. Через $\{A_w\}$ обозначается множество значений $w(x)$. Под набором $w^*=\big(w_0^*,w_1^*\dots,w_{2^n-1}^*\big)$ понимается набор упорядоченных по неубыванию элементов множества A_w. В тексте без особых оговорок используются обозначения из [2] для линейных булевых пороговых функций, которые без изменения переносятся на полиномиальный случай. В частности, факт, что к.б.п.ф. задаётся квадратичной формой q и порогом t, для краткости записывается как $f\sim(q,t)$. Имея две квадратичные формы от независимых переменных — $p(x)$ и $q(y)$, можно составить новую квадратичную форму $h(x,y)=p(x)+q(y)$ (будем обозначать $h=p|q$).

Рассмотрим бинарное отношение частичного порядка на множестве действительных квадратичных форм. Если q^* является подпоследовательностью r^* для квадратичных форм $q(x)$ и $r(y)$ (возможно, от разного числа переменных, но все переменные из x входят в y), то будем обозначать этот факт как $q\prec r$. В дальнейшем без ограничения общности будем полагать все веса целыми числами. Важность введённого бинарного отношения по отношению к изучению функциональной структуры к.б.п.ф. следует из следующего утверждения.

Утверждение 1 [2]. Пусть к.б.п.ф. $f\sim(p_1|q_1,t)$ и $g\sim(p_2|q_2,t)$ удовлетворяют свойству $p_1\prec p_2$, $q_1\prec q_2$. Тогда если g допускает простую декомпозицию, то и f допускает простую декомпозицию.

Под нетривиальной простой декомпозицией понимается следующая бесповторная суперпозиция для некоторого $m\in\{2,\dots,n-1\}$:

$$f(x_1,\dots,x_n)=\varphi\big(\psi(x_1,\dots,x_m),x_{m+1},\dots,x_n\big).$$

Утверждение 1 позволяет предложить способ построения классов функционально разделимых (или функционально неразделимых) к.б.п.ф., равно как и подход к анализу функциональной разделимости заданной к.б.п.ф. Пусть $\{u_i\}$ и $\{v_i\}$ — множества

квадратичных форм от m_i и n_i переменных ($m_i, n_i > 1$), имеющие верхние грани u и v относительно введённого бинарного отношения. Тогда если пороговая функция со структурой $(u|v,t)$ функционально разделима, то и любая пороговая функция со структурой $(u_i|v_i,t)$ также функционально разделима. Справедливо и отрицание этого утверждения.

Замечание 1. Утверждение 1 и вышеприведённые рассуждения не зависят от вида неравенства, задающего пороговую функцию, и поэтому справедливы для полиномиальных пороговых функций.

Для целочисленной матрицы W квадратичной формы определим *троичное представление* — матрицу $U^W = (u^W_{ij})_{i,j=1,\dots,N}$ некоторой квадратичной формы u^W, задаваемую следующим образом. Элементу w_{ij} матрицы W в матрице U^W соответствует клетка размера $l_i \times l_j$, причём клетки не пересекаются и расположены в том же порядке, что и сами элементы w_{ij} в матрице W. Натуральные числа l_i, $i = 1, \dots, n$, удовлетворяют условиям

$$\begin{cases} l_i l_j \geqslant |w_{ij}|, \\ N = \sum\limits_{i=1}^{n} l_i \to \min. \end{cases} \tag{2}$$

В каждой клетке произвольным образом (с сохранением свойства симметричности матрицы U^W) расставляются единицы в случае $w_{ij} > 0$ и -1 для $w_{ij} < 0$. Остальные элементы полагаются равными нулю. Троичное представление всегда существует, например, можно положить $l_i = \max\limits_{j\in\{1,\dots,n\}} w_{ij}$, хотя в этом случае условие минимальности размера N троичного представления не обязательно выполняется. Несмотря на то, что минимизация размера N полезна в практическом смысле, использование троичного представления не связано строго с этим свойством, поэтому в дальнейшем под троичным представлением также будем понимать и неоптимальные по размеру матрицы.

Дополнительный способ сокращения размера троичного представления связан с переходом к матрице $\tilde{W} = \dfrac{1}{d}W$, где $d = \text{НОД}\{w_{ij}\}$.

Задача (2) относится к задачам целочисленного квадратичного программирования с линейной целевой функцией. Путём перехода к величинам $r_i = \log l_i$ эта задача приобретает вид задачи линейного программирования в дискретной решётке $\log \mathbb{N}$. Для решения последней задачи с учётом необязательности выполнения требования оптимальности может быть применён полиномиальный алгоритм Хачияна [3] с последующим «округлением» результата в ближайший узел решётки. Отсутствие требования оптимальности делает возможным использование приближённых алгоритмов решения задачи целочисленного программирования [4, 5].

Из определения троичного представления и предшествующих рассуждений следует его неоднозначность. Другое важное свойство заключается в том, что если для булева вектора $a = (a_1, \dots, a_n)$ положить компоненты булева вектора $b = (b_1, \dots, b_N)$ в соответствии с условием $a_i = 1 \Leftrightarrow b_{l_1+\dots+l_{i-1}+1} = \dots = b_{l_1+\dots+l_i} = 1$, то

$$w(a) = aWa^T = bU^W b^T \stackrel{\text{def}}{=} u^W(b). \tag{3}$$

Справедливость (3) следует из того, что серии нулей и единиц в векторе b соответствуют клеткам матрицы U^W. Следовательно, коэффициенты w_{ij}, участвующие в вычислении (т. е. индексы i и j, такие, что $a_i = a_j = 1$), соответствуют клеткам с суммарным количеством элементов равным $\operatorname{sgn}(w_{ij})|w_{ij}|$. Таким образом, доказано

Утверждение 2. Справедливы следующие отношения:
1) $w \prec u^W$;
2) $w \prec du^{\tilde{W}}$, где $d = \text{НОД}\{w_{ij}\}$.

Представляет интерес описание функциональной структуры к.б.п.ф с матрицей квадратичной формы, имеющей вид троичного представления. Для этого, в частности, рассмотрим вопрос о существенных переменных к.б.п.ф. с матрицами квадратичных форм простого вида.

Пусть $\mathbf{1}_n$ — целочисленная квадратная матрица размера n, состоящая из одних единиц. Легко видеть, что $\{A_{\mathbf{1}_n}\} = \{k^2 : k = 0, \ldots, n\}$.

Утверждение 3. К.б.п.ф. $f \sim (\mathbf{1}_n, t)$, отличная от константы, зависит существенно от всех своих переменных.

Доказательство. Так как функция f симметричная, достаточно доказать утверждение для первой переменной. Пусть для некоторого s выполняется $t \in [s^2, (s+1)^2)$. Такое $0 \leqslant s \leqslant n-1$ существует всегда, так как по условию $0 \leqslant t < n^2$. Тогда выполняются неравенства $w(0, a) = s^2 \leqslant t$ и $w(1, a) = s^2 + 2n - 1 \geqslant (s+1)^2 > t$, где a — произвольный вектор размера $n-1$ с весом s. ■

Рассмотрим структурные свойства к.б.п.ф. $f \sim (\mathbf{1}_m | \mathbf{1}_{n-m}, t)$, где $1 \leqslant m \leqslant n-1$.

Утверждение 4. К.б.п.ф. $f \sim (\mathbf{1}_m | \mathbf{1}_{n-m}, t)$ зависит существенно от первых m $(1 \leqslant m \leqslant n-1)$ переменных, если и только если найдутся такие $r \in \{0, \ldots, m-1\}$, $s \in \{0, \ldots, n-m\}$, что выполняется система неравенств

$$\begin{cases} r^2 + s^2 \leqslant \lfloor t \rfloor_w, \\ (r+1)^2 + s^2 \geqslant \lceil t \rceil_w, \end{cases} \tag{4}$$

где квадратичная форма $w = (\mathbf{1}_m | \mathbf{1}_{n-m})$; $\lfloor t \rfloor_w$ и $\lceil t \rceil_w$ — нижние и верхнее приближения числа t в множестве $\{A_w\}$ [2].

Доказательство. Без ограничения общности будем рассматривать существенную зависимость функции f от первой переменной. Докажем утверждение, заменив (4) на равносильную систему

$$r^2 + s^2 \leqslant t < (r+1)^2 + s^2. \tag{5}$$

Действительно, по свойствам верхнего и нижнего приближений $\lfloor t \rfloor_w \leqslant t < \lceil t \rceil_w$, поэтому из (4) следует (5). Так как $r^2 + s^2$, $(r+1)^2 + s^2 \in \{A_w\}$, то справедлива и обратная импликация.

Достаточность. Если для некоторых $r \in \{0, \ldots, m-1\}$ и $s \in \{0, \ldots, n-m\}$ выполняется (4), то значения функции f на булевых векторах $(0, u, v)$ и $(1, u, v)$ различаются, где u — произвольный вектор длины $m-1$ и веса r, а v — произвольный вектор длины $n-m$ веса s. Действительно, $w(0, u, v) = r^2 + s^2 \leqslant t < (r+1)^2 + s^2 = w(1, u, v)$.

Необходимость. Пусть от противного выполняется отрицание (5), т. е. для каждой пары (r, s) верно $t < r^2 + s^2$ или $t \geqslant (r+1)^2 + s^2$, что в силу неравенств $t < r^2 + s^2 < (r+1)^2 + s^2$ и $t \geqslant (r+1)^2 + s^2 > r^2 + s^2$ равносильно совпадению значений функции на произвольных векторах $(0, u, v)$ и $(1, u, v)$, т. е. несущественной зависимости функции f от первой переменной. ■

Следствие 1. К.б.п.ф $f \sim (\mathbf{1}_1 | \mathbf{1}_{n-1}, t)$ зависит существенно от первой переменной тогда и только тогда, когда $k^2 \leqslant t < k^2 + 1$ для некоторого $k \in \{0, \ldots, n-1\}$.

Пример 1. К.б.п.ф. $f \sim (\mathbf{1}_1|\mathbf{1}_3, 2)$ зависит несущественно от первой переменной. Её таблица истинности и многочлен Жегалкина такие же, как для пороговой функции $((1,1,1),1)$, т. е. $x_2x_3 + x_2x_4 + x_3x_4$.

Пример 2. К.б.п.ф. $g_1 \sim (\mathbf{1}_2|\mathbf{1}_3, 8)$ имеет многочлен Жегалкина $x_3x_4x_5$, хотя при порогах 7 или 9 с той же матрицей квадратичной формы соответствующие функции g_2 и g_3 зависят существенно от всех пяти переменных и имеют многочлены Жегалкина $x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_3x_4x_5 + x_1x_2x_3x_4x_5$ и $x_1x_3x_4x_5 + x_2x_3x_4x_5 + x_1x_2x_3x_4x_5$ соответственно. При этом функция g_1 является линейной пороговой со структурой $((0,0,1,1,1),2)$, а функции g_2 и g_3 — линейными пороговыми со структурами $((1,1,3,3,3),7)$ и $((1,1,3,3,3),9)$ соответственно. Кроме того, обе функции допускают декомпозиции $g_2 = x_1x_2(x_3x_4 + x_3x_5 + x_4x_5 + x_3x_4x_5)$ и $g_3 = (x_1 + x_2 + x_1x_2)x_3x_4x_5$.

Приведённые примеры показывают, что даже в случае очень простых квадратичных форм задаваемые ими к.б.п.ф. могут сильно отличаться в смысле существенной зависимости от переменных при небольших (последовательных) изменениях порога. Кроме того, интерес представляет нахождение пороговой степени (см. определение в [1]) к.б.п.ф. В заключение отметим, что даже для линейной пороговой булевой функции задача определения существенной зависимости переменной является NP-полной [6, теорема 9.26, с. 436], что повышает значимость разработки эвристических методов её решения.

ЛИТЕРАТУРА

1. *Подольский В. В.* Оценки весов персептронов (полиномиальных пороговых булевых функций): автореф. дис. ... канд. физ.-мат. наук. М.: МГУ им. М. В. Ломоносова, 2009.
2. *Шурупов А. Н.* О функциональной разделимости булевых пороговых функций // Дискретная математика. 1997. Т. 9. Вып. 2. С. 59–73.
3. *Хачиян Л. Г.* Полиномиальный алгоритм в линейном программировании // Докл. АН СССР. 1979. Т. 244. № 5. С. 1033–1096.
4. *Dreo J., Petrowski A., Siarry P., and Taillard E.* Metaheuristics for Hard Optimisation. Methods and Case Studies. Springer, 2006. 372 p.
5. *Хохлюк В. И.* Прямой метод целочисленной оптимизации. Новосибирск: Ин-т математики им. С. Л. Соболева, 2002. 38 с.
6. *Crama Y. and Hammer P.* Boolean Functions. Theory, Algorithms and Applications. Cambridge University Press, 2011.

УДК 519.7 DOI 10.17223/2226308X/8/19

О СВОЙСТВАХ МНОЖЕСТВА ЗНАЧЕНИЙ ПРОИЗВОЛЬНОЙ ВЕКТОРНОЙ БУЛЕВОЙ ФУНКЦИИ[1]

Г. И. Шушуев

Исследуются свойства множества значений производных векторной булевой функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Получены достаточные условия того, что множество всех значений производных некоторой булевой функции совпадает с $\mathbb{F}_2^n$. Этот результат связан с некоторым открытым вопросом о метрических свойствах APN-функций.

[1]Работа поддержана грантом РФФИ, проект № 15-31-20635.