ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.563+519.85+517.518.244 DOI 10.17223/20710410/68/1

О ПОРЯДКЕ ГЛАДКОСТИ НАИМЕНЬШЕГО ВОГНУТОГО ПРОДОЛЖЕНИЯ БУЛЕВОЙ ФУНКЦИИ

Д. Н. Баротов*, Р. Н. Баротов**

**Финансовый университет при Правительстве РФ, г. Москва, Россия*
***Худжандский государственный университет им. акад. Б. Гафурова, г. Худжанд, Таджикистан*

E-mail: DNBarotov@fa.ru, ruzmet.tj@mail.ru

Исследуется порядок гладкости $f_{NR}(x_1, x_2, \ldots, x_n)$ — наименьшего вогнутого продолжения на $[0,1]^n$ произвольной булевой функции $f_B(x_1, x_2, \ldots, x_n)$. Доказано, что если булева функция $f_B(x_1, x_2, \ldots, x_n)$ существенно зависит не более чем от одной переменной, то на $[0,1]^n$ её наименьшее вогнутое продолжение $f_{NR}(x_1, x_2, \ldots, x_n)$ бесконечно дифференцируемо, в противном случае продолжение $f_{NR}(x_1, x_2, \ldots, x_n)$ на $[0,1]^n$ всего лишь непрерывно. Продемонстрировано применение наименьшего вогнутого продолжения к решению систем булевых уравнений.

Ключевые слова: *вогнутое продолжение булевой функции, булева функция, вогнутая функция, глобальная оптимизация, локальный экстремум.*

ON THE ORDER OF SMOOTHNESS OF THE SMALLEST CONCAVE EXTENSION OF A BOOLEAN FUNCTION

D. N. Barotov*, R. N. Barotov**

**Financial University under the Government of the Russian Federation, Moscow, Russia*
***Khujand state university named after academician Bobojon Gafurov, Khujand, Tajikistan*

In this paper, we study the order of smoothness of $f_{NR}(x_1, x_2, \ldots, x_n)$ — the least concave extension on $[0,1]^n$ of an arbitrary Boolean function $f_B(x_1, x_2, \ldots, x_n)$. We prove that if the Boolean function $f_B(x_1, x_2, \ldots, x_n)$ essentially depends on at most one variable, then on $[0,1]^n$ its least concave extension $f_{NR}(x_1, x_2, \ldots, x_n)$ is infinitely differentiable, otherwise the extension $f_{NR}(x_1, x_2, \ldots, x_n)$ on $[0,1]^n$ is only continuous. We demonstrate how the least concave extension can be used to solve systems of Boolean equations.

Keywords: *concave extension of a Boolean function, Boolean function, concave function, global optimization, local extremum.*

Введение

Различные труднорешаемые дискретные задачи, возникающие во многих областях, включая комбинаторику, современную кибернетику, биоинформатику, автоматизацию проектирования микроэлектроники, проектирование классических логических цепей, распознавание образов, функционирование конечных автоматов специального вида, а также криптографию, могут быть сведены к системам булевых уравнений [1–5]. Поэтому, с одной стороны, решению систем булевых уравнений посвящено значительное количество работ, разработано несколько направлений исследования и алгоритмов их решения, а, с другой стороны, в связи с тем, что задача решения системы булевых уравнений в общем случае является NP-трудной, в научном сообществе продолжает расти интерес к поиску новых алгоритмов как в классических, так и в квантовых моделях вычислений [6–9]. Одним из таких направлений является то, что задача решения системы булевых уравнений, в том числе путём представления некоторого вещественного продолжения (аналога) для каждой булевой функции, преобразуется в задачу с вещественными переменными, которая может быть либо задачей оптимизации некоторой функции, что позволяет применять оптимизационные методы вычислительной математики [10–14], либо задачей MILP или QUBO, решаемой классическими дискретными алгоритмами оптимизации или квантовыми алгоритмами [15, 16], либо системой полиномиальных уравнений, решаемой на множестве целых чисел [17], либо эквивалентной системой полиномиальных уравнений, решаемой и анализируемой символьными методами [18].

Отметим, что существует много способов, каждый из которых, используя вещественное продолжение булевой функции, выбранное на основе некоторого соображения, позволяет преобразовать систему булевых уравнений в задачу непрерывной оптимизации, так как принципиальное отличие таких способов от переборных алгоритмов локального поиска состоит в том, что на каждой итерации алгоритма сдвиг по градиенту (антиградиенту) производится по всем переменным одновременно [19]. Одна из основных проблем, возникающая при применении этих способов, заключается в том, что оптимизируемая целевая функция в искомой области может иметь множество локальных экстремумов, что значительно усложняет их практическое использование [14, 20, 21].

По изложенной проблеме в [14, 20–26] получены некоторые результаты, а именно: в [14, 20] рассмотрено конструирование полилинейного продолжения булевой функции и аргументировано, что задача решения произвольной системы булевых уравнений с n переменными может быть сведена к задаче непрерывной минимизации на $[0,1]^n$ целевой функции, не имеющей строгих локальных минимумов внутри любой k-мерной грани куба $[0,1]^n$, $k \in \{1, 2, \ldots, n\}$, а в [21–25] построены выпуклые (вогнутые) продолжения булевых функций n переменных на $[0,1]^n$ и на основе построенных продолжений конструктивно доказано, что задача решения системы булевых уравнений может быть сведена к задаче минимизации (максимизации) целевой функции, любой локальный минимум (максимум) которой в искомой области является глобальным минимумом (максимумом), а также что для любой булевой функции от n переменных существует единственная вещественная функция, являющаяся максимумом (минимумом) среди всех её выпуклых (вогнутых) продолжений на $[0,1]^n$. В [26] проведено сравнительное исследование между выпуклыми, полилинейными и вогнутыми продолжениями булевых функций. Поэтому построение вещественных продолжений булевых функций, представляющих интерес при преобразовании систем булевых уравнений к задаче непрерывной оптимизации, и изучение их свойств также являются важными.

Данная работа посвящается исследованию порядка гладкости наименьшего вогнутого продолжения на $[0,1]^n$ произвольной булевой функции $f_B : \{0,1\}^n \to \{0,1\}$, представленного в [24], и является продолжением работ [14, 18, 20–26]. Установлен порядок дифференцируемости наименьшего вогнутого продолжения на $[0,1]^n$ произвольной булевой функции $f_B : \{0,1\}^n \to \{0,1\}$, а именно: во-первых, оценивая наименьшее вогнутое продолжение на $[0,1]^n$ произвольной булевой функции $f_B(x)$ с обеих сторон, доказано, что оно непрерывно на $[0,1]^n$; во-вторых, доказано, что если число существенных переменных булевой функции $f_B(x)$ меньше двух, то наименьшее вогнутое продолжение является бесконечно дифференцируемым, а иначе — лишь непрерывным.

1. Используемые определения и обозначения

Пусть $\mathbb{B}^n = \{(b_1,\ldots,b_n) : b_1,\ldots,b_n \in \{0,1\}\}$ — множество всевозможных двоичных слов (булевых векторов) длины n; $\mathbb{K}^n = \{(x_1,\ldots,x_n) : x_1,\ldots,x_n \in [0,1]\}$ — n-мерный куб, натянутый на булевы векторы длины n; $\operatorname{int}(\mathbb{K}^n) = \{(x_1,\ldots,x_n) : x_1,\ldots,x_n \in (0,1)\}$ — множество внутренних точек куба $\mathbb{K}^n$.

Определение 1. Отображение вида $f_B : \mathbb{B}^n \to \{0,1\}$ называется булевой функцией.

Определение 2. Переменная x_k, $k \in \{1,\ldots,n\}$, булевой функции $f_B(x_1,\ldots,x_n)$ называется существенной (функция $f_B(x_1,x_2,\ldots,x_n)$ существенно зависит от x_k), если

$$f_B(x_1,\ldots,x_{k-1},0,x_{k+1},\ldots,x_n) \not\equiv f_B(x_1,\ldots,x_{k-1},1,x_{k+1},\ldots,x_n).$$

Пусть
$$\mathbf{\Lambda}(x_1,x_2,\ldots,x_n) = \Big\{ \big(\lambda_{(0,0,\ldots,0)}, \lambda_{(0,0,\ldots,1)}, \ldots, \lambda_{(1,1,\ldots,1)}\big) \in \mathbb{K}^{2^n} : \sum_{(b_1,b_2,\ldots,b_n)\in\mathbb{B}^n} \lambda_{(b_1,b_2,\ldots,b_n)}(b_1,b_2,\ldots,b_n,1) = (x_1,x_2,\ldots,x_n,1)\Big\}$$

— множество весовых коэффициентов, используемых для представления точки $(x_1,x_2,\ldots,x_n)$ в виде выпуклой комбинации вершин куба $\mathbb{K}^n$.

Определение 3. Отображение вида $f : \mathbb{K}^n \to \mathbb{R}$ называется вогнутой функцией на $\mathbb{K}^n$, если для любых $x, y \in \mathbb{K}^n$ и любого $\alpha \in [0,1]$ выполняется

$$f(\alpha\, x + (1-\alpha)y) \geqslant \alpha\, f(x) + (1-\alpha) f(y).$$

Определение 4. Отображение вида $f_C : \mathbb{K}^n \to \mathbb{R}$ назовём вогнутым продолжением на $\mathbb{K}^n$ булевой функции $f_B : \mathbb{B}^n \to \mathbb{B}$, если выполняются следующие два условия:

1) отображение f_C на $\mathbb{K}^n$ является вогнутой функцией;
2) имеет место равенство $f_C(b_1,\ldots,b_n) = f_B(b_1,\ldots,b_n)$ для всех $(b_1,\ldots,b_n) \in \mathbb{B}^n$.

Определение 5. Отображение вида $f_{NR} : \mathbb{K}^n \to \mathbb{R}$ назовём наименьшим среди всех вогнутых продолжений на $\mathbb{K}^n$ булевой функции $f_B : \mathbb{B}^n \to \mathbb{B}$, если выполняются следующие два условия:

1) отображение f_{NR} является вогнутым продолжением булевой функции f_B на $\mathbb{K}^n$;
2) для любого f_C — вогнутого продолжения на $\mathbb{K}^n$ булевой функции f_B — и любого $(x_1,\ldots,x_n) \in \mathbb{K}^n$ справедливо неравенство $f_{NR}(x_1,\ldots,x_n) \leqslant f_C(x_1,\ldots,x_n)$.

2. Установление порядка дифференцируемости наименьшего вогнутого продолжения на $\mathbb{K}^n$ произвольной булевой функции

Лемма 1. Для каждой булевой функции $f_B(x_1,x_2)$, которая существенно зависит от переменных x_1 и x_2, справедливо неравенство

$$f_B(0,0) - f_B(0,1) - f_B(1,0) + f_B(1,1) \neq 0. \tag{1}$$

Доказательство. Переменные x_1 и x_2 являются существенными для булевой функции $f_B(x_1, x_2)$ тогда и только тогда, когда

$$\begin{gathered}(f_B(0,0), f_B(0,1), f_B(1,0), f_B(1,1)) \in \big\{(0,0,0,1),(0,0,1,0),(0,1,0,0),\\ (0,1,1,0),(0,1,1,1),(1,0,0,0),(1,0,0,1),(1,0,1,1),(1,1,0,1),(1,1,1,0)\big\}.\end{gathered} \tag{2}$$

Легко заметить, что из (2) следует справедливость (1). ■

В [24] доказано, что для произвольной булевой функции $f_B(x_1, \ldots, x_n)$ вещественная функция

$$f_{NR}(x_1, \ldots, x_n) = \max_{\lambda \in \mathbf{\Lambda}(x_1,\ldots,x_n)} \left[\sum_{(b_1,\ldots,b_n) \in \mathbb{B}^n} \lambda_{(b_1,\ldots,b_n)} f_B(b_1, \ldots, b_n) \right] \tag{3}$$

является единственным наименьшим среди всех её вогнутых продолжений на $\mathbb{K}^n$.

Вообще говоря, ограниченная вогнутая (выпуклая) функция, определённая на множестве $\mathbb{K}^n$, непрерывна во внутренних точках множества $\mathbb{K}^n$ и разрывна в его граничных точках. В качестве иллюстрирующего примера приведём вещественную разрывную вогнутую функцию

$$f_C(x) = \begin{cases} 0, & \text{если } x \in \{0,1\},\\ 1, & \text{если } x \in (0,1),\end{cases}$$

которая также является вогнутым продолжением на $[0,1]$ булевой функции $f_B(x) = 0$. Но в нашем случае вещественная функция $f_{NR}(x_1, \ldots, x_n)$, являющаяся наименьшим вогнутым продолжением на $\mathbb{K}^n$ булевой функции $f_B(x_1, \ldots, x_n)$, непрерывна на $\mathbb{K}^n$ для каждого натурального n. Ниже, ради полноты изложения, путём построения двусторонней оценки мы предъявим полное доказательство непрерывности $f_{NR}(x_1, \ldots, x_n)$ для произвольного натурального n и установим порядок дифференцируемости $f_{NR}(x_1, \ldots, x_n)$.

Теорема 1. Функция $f_{NR}(x_1, \ldots, x_n)$, определённая формулой (3), на $\mathbb{K}^n$ непрерывна.

Доказательство. Индукция по n.

База индукции. Согласно [24, следствия 1 и 2], имеем, что, во-первых, для любой булевой функции $f_B(x)$, зависящей от одной переменной, вещественная функция

$$f_{NR}(x) = (1-x) f_B(0) + x\, f_B(1) \tag{4}$$

является единственным наименьшим среди всех её вогнутых продолжений на $\mathbb{K}$; во-вторых, для любой булевой функции $f_B(x,y)$, зависящей от двух переменных, вещественная функция вида

$$\begin{gathered} f_{NR}(x,y) = (1-x-y) f_B(0,0) + x\, f_B(1,0) + y\, f_B(0,1) + \\ + \frac{f_B(0,0) - f_B(0,1) - f_B(1,0) + f_B(1,1)}{4}(2x + 2y - 1 - |x-y| + |x+y-1|) - \\ - \frac{|f_B(0,0) - f_B(0,1) - f_B(1,0) + f_B(1,1)|}{4}(|x-y| + |x+y-1| - 1) \end{gathered} \tag{5}$$

является единственным наименьшим среди всех её вогнутых продолжений на $\mathbb{K}^2$. Непрерывность функций $f_{NR}(x)$ и $f_{NR}(x,y)$, ввиду (4) и (5), очевидна.

П р е д п о л о ж е н и е и н д у к ц и и . Пусть при $n = k$ для произвольной булевой функции $f_B(x_1, \ldots, x_k)$ наименьшее вогнутое продолжение $f_{NR}(x_1, \ldots, x_k)$ непрерывно на $\mathbb{K}^k$.

Ш а г и н д у к ц и и . Докажем, что функция $f_{NR}(x_1, \ldots, x_{k+1})$, являющаяся наименьшим вогнутым продолжением на $\mathbb{K}^{k+1}$ булевой функции $f_B(x_1, \ldots, x_{k+1})$, непрерывна на $\mathbb{K}^{k+1}$. Пусть $(x_1^*, \ldots, x_{k+1}^*)$ — произвольная точка куба $\mathbb{K}^{k+1}$. Покажем, что имеет место равенство

$$\lim_{(\Delta x_1, \ldots, \Delta x_{k+1}) \to (0, \ldots, 0)} f_{NR}(x_1^* + \Delta x_1, \ldots, x_{k+1}^* + \Delta x_{k+1}) = f_{NR}(x_1^*, \ldots, x_{k+1}^*). \tag{6}$$

Рассмотрим два случая.

С л у ч а й 1 . Пусть $(x_1^*, \ldots, x_{k+1}^*) \in \operatorname{int}(\mathbb{K}^{k+1})$. Ввиду открытости множества $\operatorname{int}(\mathbb{K}^{k+1})$ доказательство можно провести по известной схеме, например [27].

С л у ч а й 2 . Пусть $(x_1^*, \ldots, x_{k+1}^*) \in \partial(\mathbb{K}^{k+1}) = \mathbb{K}^{k+1} \setminus \operatorname{int}(\mathbb{K}^{k+1})$. Тогда существует $i \in \{1, \ldots, k+1\}$, такое, что $x_i^* \in \{0, 1\}$. Согласно предположению индукции, функции, полученные путём сужения, вида

$$\begin{gathered} f_0(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k+1}) = f_{NR}(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_{k+1}) = \\ = \max_{\substack{\lambda \in \boldsymbol{\Lambda}(x_1, \ldots, x_{i-1}, \\ x_{i+1}, \ldots, x_{k+1})}} \Bigg[\sum_{\substack{(b_1, \ldots, b_{i-1}, \\ b_{i+1}, \ldots, b_{k+1}) \in \mathbb{B}^k}} \lambda_{(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_{k+1})} f_B(b_1, \ldots, b_{i-1}, 0, b_{i+1}, \ldots, b_{k+1}) \Bigg] \end{gathered} \tag{7}$$

и

$$\begin{gathered} f_1(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k+1}) = f_{NR}(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_{k+1}) = \\ = \max_{\substack{\lambda \in \boldsymbol{\Lambda}(x_1, \ldots, x_{i-1}, \\ x_{i+1}, \ldots, x_{k+1})}} \Bigg[\sum_{\substack{(b_1, \ldots, b_{i-1}, \\ b_{i+1}, \ldots, b_{k+1}) \in \mathbb{B}^k}} \lambda_{(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_{k+1})} f_B(b_1, \ldots, b_{i-1}, 1, b_{i+1}, \ldots, b_{k+1}) \Bigg] \end{gathered} \tag{8}$$

непрерывны на $\mathbb{K}^k$. Докажем, что вещественная непрерывная функция вида

$$\begin{gathered} g(x_1, \ldots, x_{k+1}) = \min(1 - x_i, f_0(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k+1})) + \\ + \min(x_i, f_1(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k+1})) \end{gathered} \tag{9}$$

является вогнутым продолжением на $\mathbb{K}^{k+1}$ булевой функции $f_B(x_1, \ldots, x_{k+1})$. Для этого достаточно показать справедливость следующих двух свойств:

1) $g(b_1, \ldots, b_{k+1}) = f_B(b_1, \ldots, b_{k+1})$ для всех $(b_1, \ldots, b_{k+1}) \in \mathbb{B}^{k+1}$;

2) функция $g(x_1, \ldots, x_{k+1})$ на $\mathbb{K}^{k+1}$ является вогнутой.

Обоснуем эти свойства:

1) Для всех $(b_1, \ldots, b_{k+1}) \in \mathbb{B}^{k+1}$ имеем

$$\begin{gathered} g(b_1, \ldots, b_{k+1}) = \min(1 - b_i, f_0(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_{k+1})) + \\ + \min(b_i, f_1(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_{k+1})) = \\ = (1 - b_i) f_0(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_{k+1}) + b_i\, f_1(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_{k+1}) = \\ = (1 - b_i) f_{NR}(b_1, \ldots, b_{i-1}, 0, b_{i+1}, \ldots, b_{k+1}) + b_i\, f_{NR}(b_1, \ldots, b_{i-1}, 1, b_{i+1}, \ldots, b_{k+1}) = \\ = \overline{b_i}\, f_{NR}(b_1, \ldots, b_{i-1}, 0, b_{i+1}, \ldots, b_{k+1}) \oplus b_i\, f_{NR}(b_1, \ldots, b_{i-1}, 1, b_{i+1}, \ldots, b_{k+1}) = f_B(b_1, \ldots, b_{k+1}). \end{gathered}$$

2) Функции $f_0(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k+1})$ и $f_1(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k+1})$, ввиду (7) и (8), на $\mathbb{K}^k$ являются вогнутыми и, следовательно, для любых $x, y \in \mathbb{K}^{k+1}$ и любого $\alpha \in [0, 1]$ имеем

$$g(\alpha x + (1 - \alpha) y) = \min\big(1 - (\alpha x_i + (1 - \alpha) y_i), f_0(\alpha x_1 + (1 - \alpha) y_1, \ldots, \alpha x_{i-1} + (1 - \alpha) y_{i-1},$$

$$\alpha x_{i+1}+(1-\alpha)y_{i+1},\dots,\alpha x_{k+1}+(1-\alpha)y_{k+1})\big)+\min\big(\alpha x_i+(1-\alpha)y_i, f_1(\alpha x_1+(1-\alpha)y_1,\\ \dots,\alpha x_{i-1}+(1-\alpha)y_{i-1},\alpha x_{i+1}+(1-\alpha)y_{i+1},\dots,\alpha x_{k+1}+(1-\alpha)y_{k+1})\big)\geqslant\\ \geqslant\min\big(\alpha(1-x_i)+(1-\alpha)(1-y_i),\alpha f_0(x_1,\dots,x_{i-1},x_{i+1},\dots,x_{k+1})+\\ +(1-\alpha)f_0(y_1,\dots,y_{i-1},y_{i+1},\dots,y_{k+1})\big)+\min\big(\alpha x_i+(1-\alpha)y_i,\\ \alpha f_1(x_1,\dots,x_{i-1},x_{i+1},\dots,x_{k+1})+(1-\alpha)f_1(y_1,\dots,y_{i-1},y_{i+1},\dots,y_{k+1})\big)\geqslant\\ \geqslant\alpha\min(1-x_i,f_0(x_1,\dots,x_{i-1},x_{i+1},\dots,x_{k+1}))+(1-\alpha)\min(1-y_i,f_0(y_1,\dots,y_{i-1},y_{i+1},\\ \dots,y_{k+1}))+\alpha\min(x_i,f_1(x_1,\dots,x_{i-1},x_{i+1},\dots,x_{k+1}))+\\ +(1-\alpha)\min(y_i,f_1(y_1,\dots,y_{i-1},y_{i+1},\dots,y_{k+1}))=\alpha g(x)+(1-\alpha)g(y).$$

Далее, с одной стороны, ввиду определения наименьшего вогнутого продолжения, для $(x^*+\Delta x)\in\mathbb{K}^{k+1}$ выполняется

$$f_{NR}(x^*+\Delta x)-f_{NR}(x^*)\leqslant g(x^*+\Delta x)-f_{NR}(x^*), \tag{10}$$

а, с другой стороны, ввиду вогнутости функции $f_{NR}(x)$, для $(x^*+\Delta x)\in\mathbb{K}^{k+1}$ имеем

$$\begin{gathered}f_{NR}(x^*+\Delta x)-f_{NR}(x^*)=f_{NR}\big((1-(1-2x_i^*)\Delta x_i)(x_1^*+\Delta x_1,\dots,x_{i-1}^*+\Delta x_{i-1},\\ x_i^*,x_{i+1}^*+\Delta x_{i+1},\dots,x_{k+1}^*)+(1-2x_i^*)\Delta x_i(x_1^*+\Delta x_1,\dots,x_{i-1}^*+\Delta x_{i-1},1-x_i^*,\\ x_{i+1}^*+\Delta x_{i+1},\dots,x_{k+1}^*)\big)-f_{NR}(x^*)\geqslant\\ \geqslant(1-(1-2x_i^*)\Delta x_i)f_{NR}(x_1^*+\Delta x_1,\dots,x_{i-1}^*+\Delta x_{i-1},x_i^*,x_{i+1}^*+\Delta x_{i+1},\dots,x_{k+1}^*)+\\ +(1-2x_i^*)\Delta x_i\, f_{NR}(x_1^*+\Delta x_1,\dots,x_{i-1}^*+\Delta x_{i-1},1-x_i^*,\\ x_{i+1}^*+\Delta x_{i+1},\dots,x_{k+1}^*)-f_{NR}(x^*).\end{gathered} \tag{11}$$

Ввиду (9) и непрерывности функций $f_0(x_1,\dots,x_{i-1},x_{i+1},\dots,x_{k+1})$ и $f_1(x_1,\dots,x_{i-1},x_{i+1},\dots,x_{k+1})$, переходя к пределу в оценках (10) и (11) при $(\Delta x_1,\dots,\Delta x_{k+1})\to\to(0,\dots,0)$, получим (6). ■

Теорема 2. Если у булевой функции $f_B(x_1,\dots,x_n)$ не меньше двух существенных переменных, то вещественная функция $f_{NR}(x_1,\dots,x_n)$, которая является её наименьшим вогнутым продолжением на $\mathbb{K}^n$, не дифференцируема на $\mathbb{K}^n$.

Доказательство. Не теряя общности, будем считать, что все переменные функции $f_B(x_1,\dots,x_n)$ являются существенными. Докажем от противного: пусть вещественная функция $f_{NR}(x_1,\dots,x_n)$, которая является наименьшим вогнутым продолжением на $\mathbb{K}^n$ булевой функции $f_B(x_1,\dots,x_n)$, является дифференцируемой в каждой точке $(x_1^*,\dots,x_n^*)$ куба $\mathbb{K}^n$ при $n\geqslant 2$. Тогда для всех $(b_1,\dots,b_{i-1},b_{i+1},\dots,b_{j-1},b_{j+1},\dots,b_n)\in\mathbb{B}^{n-2}$ суженная вещественная функция $f_{NR}(b_1,\dots,b_{i-1},x_i,b_{i+1},\dots,b_{j-1},x_j,b_{j+1},\dots,b_n)$ является дифференцируемой в каждой точке (x_i^*,x_j^*) квадрата $\mathbb{K}^2$. Согласно [28], существует $(b_1^*,\dots,b_{i-1}^*,b_{i+1}^*,\dots,b_{j-1}^*,b_{j+1}^*,\dots,b_n^*)\in\mathbb{B}^{n-2}$, такой, что переменные x_i и x_j суженной булевой функции $f_B(b_1^*,\dots,b_{i-1}^*,x_i,b_{i+1}^*,\dots,b_{j-1}^*,x_j,b_{j+1}^*,\dots,b_n^*)$ являются существенными. Отсюда получим, что вещественная функция

$$g_{NR}(x_i,x_j)=f_{NR}(b_1^*,\dots,b_{i-1}^*,x_i,b_{i+1}^*,\dots,b_{j-1}^*,x_j,b_{j+1}^*,\dots,b_n^*),$$

которая является наименьшим вогнутым продолжением на $\mathbb{K}^2$ булевой функции

$$g_B(x_i,x_j)=f_B(b_1^*,\dots,b_{i-1}^*,x_i,b_{i+1}^*,\dots,b_{j-1}^*,x_j,b_{j+1}^*,\dots,b_n^*),$$

является дифференцируемой в каждой точке (x_i^*, x_j^*) квадрата $\mathbb{K}^2$. Теперь, с одной стороны, ввиду леммы 1, имеем, что

$$g_B(0,0) - g_B(0,1) - g_B(1,0) + g_B(1,1) \neq 0, \tag{12}$$

а, с другой стороны, ввиду [24, следствие 2], получаем

$$\begin{gathered} g_{NR}(x_i,x_j) = (1-x_i-x_j)g_B(0,0)+x_i\, g_B(1,0)+x_j\, g_B(0,1)+ \\ +\frac{g_B(0,0)-g_B(0,1)-g_B(1,0)+g_B(1,1)}{4}\,(2x_i+2x_j-1-|x_i-x_j|+|x_i+x_j-1|)- \\ -\frac{|g_B(0,0)-g_B(0,1)-g_B(1,0)+g_B(1,1)|}{4}\,(|x_i-x_j|+|x_i+x_j-1|-1). \end{gathered} \tag{13}$$

В силу (12) из (13) следует, что функция $g_{NR}(x_i,x_j)$ не является дифференцируемой на $\mathbb{K}^2$, т. е. не является дифференцируемой в каждой точке (x_i^*, x_j^*) квадрата $\mathbb{K}^2$. Полученное противоречие завершает доказательство теоремы 2. ■

Проиллюстрируем одно из возможных применений наименьшего вогнутого продолжения к решению систем булевых уравнений на примере системы из двух уравнений

$$\begin{cases} p_1(x,y) = x\cdot y \oplus x = 1, \\ p_2(x,y) = x \oplus y = 1, \end{cases} \tag{14}$$

приведённой в [14], т. е. проиллюстрируем общий метод, развитый в [24]. Систему (14) на основе (5) преобразуем в систему вогнутых уравнений вида

$$\begin{cases} f_1(x,y) = \dfrac{1}{2}\,(x-y+1-|x+y-1|) = 1, \\ f_2(x,y) = 1-|x+y-1| = 1, \end{cases} \tag{15}$$

где $f_k(x,y)$ — наименьшее вогнутое продолжение на $\mathbb{K}^2$ функции $p_k(x,y)$, $k \in \{1,2\}$. В свою очередь, для системы (15) конструируем максимизируемую вогнутую целевую функцию вида

$$f(x,y) = f_1(x,y) + f_2(x,y). \tag{16}$$

Ввиду (3) имеем, что для всех $(x,y) \in \mathbb{K}^2$ и $k \in \{1,2\}$ имеют место неравенства

$$0 \leqslant f_k(x,y) \leqslant 1. \tag{17}$$

Из (16) и (17) получаем, что $(x^*,y^*) \in \mathbb{K}^2$ — решение системы (15) тогда и только тогда, когда $\max\limits_{(x,y)\in\mathbb{K}^2} f(x,y) = f(x^*,y^*) = 2$. На рис. 1 приведён график функции $f(x,y)$; нетрудно заметить, что $(x^*,y^*) = (1,0)$ — единственная точка максимума функции $f(x,y)$ на $\mathbb{K}^2$.

Отметим, что если при преобразовании для каждой булевой функции брать в качестве вогнутого продолжения не наименьшее, а, например,

$$\tilde{f}_1(x,y) = \frac{1}{2}(x-y-|x-y|)+1-|x-1+y| \quad \text{и} \quad \tilde{f}_2(x,y) = 1-|x+y-1|,$$

то система вогнутых уравнений

$$\begin{cases} \tilde{f}_1(x,y) = 1, \\ \tilde{f}_2(x,y) = 1 \end{cases} \tag{18}$$

будет иметь решение, не являющееся решением булевой системы (14), т. е. целевая функция

$$\tilde{f}(x,y) = \tilde{f}_1(x,y) + \tilde{f}_2(x,y)$$

имеет точку максимума, например $(3/4, 1/4)$, которая является решением системы (18), но не является решением булевой системы (14) (рис. 2).

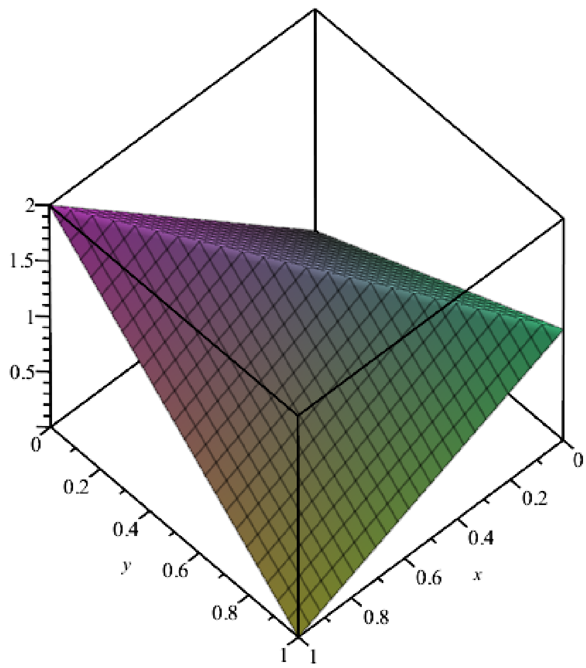

Рис. 1. График функции $f(x,y)$

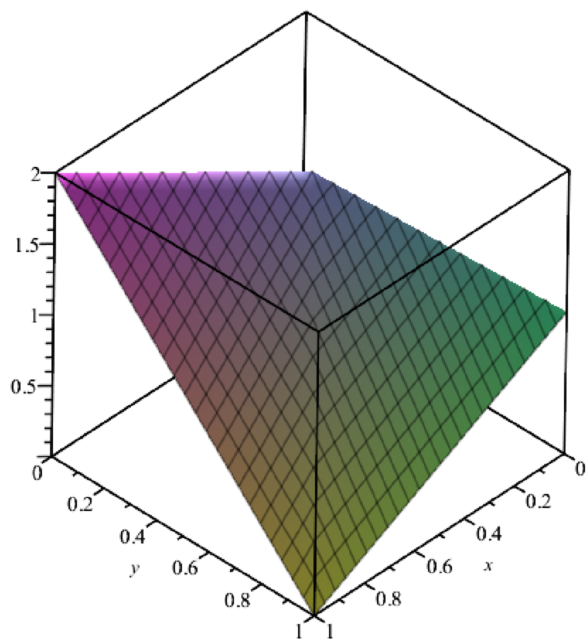

Рис. 2. График функции $\tilde{f}(x,y)$

Заключение

Таким образом, ввиду формулы (4) и теорем 1 и 2 имеем, что если число существенных переменных произвольной булевой функции не меньше двух, то её наименьшее вогнутое продолжение на $\mathbb{K}^n$ непрерывно, но не дифференцируемо на $\mathbb{K}^n$, а если меньше двух, то линейно и, следовательно, бесконечно дифференцируемо на $\mathbb{K}^n$.

Авторы выражают благодарность рецензентам за полезные замечания, исправление которых позволило улучшить содержание статьи.

ЛИТЕРАТУРА

1. *Заикин О. С., Семёнов А. А., Посыпкин М. А.* Процедуры построения декомпозиционных множеств для распределенного решения SAT-задач в проекте добровольных вычислений SAT@home // Управление большими системами. 2013. Вып. 43. С. 138–156.
2. *Заикин О. С., Семенов А. А.* Применение метода Монте-Карло к прогнозированию времени параллельного решения проблемы булевой выполнимости // Выч. мет. программирование. 2014. Т. 15. №1. С. 22–35.
3. *Мальцева М. А., Румянцев А. С.* Проверка выполнимости булевых формул с помощью квантового отжига // Труды Карельского научного центра РАН. 2023. №4. С. 41–49.
4. *Леонтьев В. К., Нурлыбаев А. Н.* Об одном классе систем булевых уравнений // Ж. вычисл. матем. и матем. физ. 1975. Т. 15. №6. С. 1568–1579.
5. *Леонтьев В. К., Тоноян Г. П.* О системах булевых уравнений // Ж. вычисл. матем. и матем. физ. 2013. Т. 53. №5. С. 800–807.

6. *Ramos-Calderer S., Bravo-Prieto C., Lin R., et al.* Solving systems of Boolean multivariate equations with quantum annealing // Phys. Rev. Res. 2022. V. 4. No. 1. Paper 013096.
7. *Bennakhi A., Byrd G. T., and Franzon P.* Solving the B-SAT problem using quantum computing: Smaller is sometimes better // Entropy. 2024. V. 26. No. 10. Paper 875.
8. *Леонтьев В. К., Тоноян Г. П.* Приближенные решения систем булевых уравнений // Ж. вычисл. матем. и матем. физ. 1993. Т. 33. № 9. С. 1383–1390.
9. *Леонтьев В. К., Гордеев Э. Н.* О числе решений системы булевых уравнений // Автомат. и телемех. 2021. № 9. С. 150–168.
10. *Gu J.* How to Solve Very Large-Scale Satisfiability (VLSS) Problems. Technical Report UCECETR-90-002. Calgary: University of Calgary, 1990.
11. *Gu J.* On optimizing a search problem // N. G. Burbakis (ed). Artificial Intelligence Methods and Applications. 1992. P. 63–105.
12. *Gu J.* Global optimization for satisfiability (SAT) problem // IEEE Trans. Knowledge Data Engin. 1994. V. 6. No. 3. P. 361–381.
13. *Gu J., Gu Q., and Du D.* On optimizing the satisfiability (SAT) problem // J. Computer Sci. Technology. 1999. V. 14. No. 1. P. 1–17.
14. *Barotov D. N.* Target function without local minimum for systems of logical equations with a unique solution // Mathematics. 2022. V. 10. No. 12:2097.
15. *Pakhomchik A. I., Voloshinov V. V., Vinokur V. M., and Lesovik G. B.* Converting of Boolean expression to linear equations, inequalities and QUBO penalties for cryptanalysis // Algorithms. 2022. V. 15. No. 2:33.
16. *Burek E., Wronski M., Mank K., and Misztal M.* Algebraic attacks on block ciphers using quantum annealing // IEEE Trans. Emerging Topics in Computing. 2022. V. 10. No. 2. P. 678–689.
17. *Abdel-Gawad A. H., Atiya A. F., and Darwish N. M.* Solution of systems of Boolean equations via the integer domain // Inform. Sci. 2010. V. 180. No. 2. P. 288–300.
18. *Barotov D. N., Barotov R. N., Soloviev V., et al.* The development of suitable inequalities and their application to systems of logical equations // Mathematics. 2022. V. 10. No. 11:1851.
19. *Файзуллин Р. Т., Дулькейт В. И., Огородников Ю. Ю.* Гибридный метод поиска приближенного решения задачи 3-выполнимость, ассоциированной с задачей факторизации // Труды Института математики и механики УрО РАН. 2013. Т. 19. № 2. С. 285–294.
20. *Баротов Д. Н., Баротов Р. Н.* Полилинейные продолжения некоторых дискретных функций и алгоритм их нахождения // Выч. мет. программирование. 2023. Т. 24. № 1. С. 10–23.
21. *Баротов Д. Н., Баротов Р. Н.* Конструирование гладких выпуклых продолжений булевых функций // Вестник российских университетов. Математика. 2024. Т. 29. № 145. С. 20–28.
22. *Баротов Д. Н.* Выпуклое продолжение булевой функции и его приложения // Дискрет. анализ исслед. опер. 2024. Т. 31. № 1. С. 5–18.
23. *Баротов Д. Н.* О существовании и свойствах выпуклых продолжений булевых функций // Матем. заметки. 2024. Т. 115. № 4. С. 533–551.
24. *Баротов Д. Н.* Вогнутые продолжения булевых функций и некоторые их свойства и приложения // Изв. Иркут. ун-та. Сер. Математика. 2024. Т. 49. С. 105–123.
25. *Баротов Д. Н.* Выпуклые продолжения некоторых дискретных функций // Дискрет. анализ исслед. опер. 2024. Т. 31. № 3. С. 5–23.
26. *Баротов Д. Н., Судаков В. А.* О неравенствах между выпуклыми, вогнутыми и полилинейными продолжениями булевых функций // Препринты ИПМ им. М. В. Келдыша. 2024. № 30. С. 1–13.

27. *Экланд И., Темам Р.* Выпуклый анализ и вариационные проблемы. М.: Мир, 1979. 399 с.
28. *Salomaa A.* On essential variables of functions, especially in the algebra of logic // Ann. Acad. Sci. Fenn. Ser. AI Math. 1963. No. 339. P. 1–11.
29. *Jensen J. L. W. V.* Sur les fonctions convexes et les inegalites entre les valeurs moyennes // Acta Mathematica. 1906. V. 30. No. 1. P. 175–193.

REFERENCES

1. *Zaikin O. S., Semenov A. A., and Posypkin M. A.* Protsedury postroeniya dekompozitsionnykh mnozhestv dlya raspredelennogo resheniya SAT-zadach v proekte dobrovol'nykh vychisleniy SAT@home [Constructing decomposition sets for distributed solution of SAT problems in volunteer computing project SAT@home]. Upravlenie Bol'shimi Sistemami, 2013, iss. 43, pp. 138–156. (in Russian)
2. *Zaikin O. S. and Semenov A. A.* Primenenie metoda Monte-Karlo k prognozirovaniyu vremeni parallel'nogo resheniya problemy bulevoy vypolnimosti [Application of the Monte Carlo method for estimating the total time of solving the SAT problem in parallel]. Vychislitel'nye Metody i Programmirovanie, 2014, vol. 15, no. 1, pp. 22–35. (in Russian)
3. *Maltseva M. A. and Rumyantsev A. S.* Proverka vypolnimosti bulevykh formul s pomoshch'yu kvantovogo otzhiga [Boolean satisfiability verification by quantum annealing]. Trudy Karel'skogo nauchnogo tsentra RAN, 2023, no. 4, pp. 41–49. (in Russian)
4. *Leont'ev V. K. and Nurlybaev A. N.* A certain class of systems of Boolean equations. U.S.S.R. Comput. Math. Math. Phys., 1975, vol. 15, no. 6, pp. 198–210.
5. *Leont'ev V. K. and Tonoyan G. P.* On systems of Boolean equations. Comput. Math. Math. Phys., 2013, vol. 53, no. 5, pp. 632–639.
6. *Ramos-Calderer S., Bravo-Prieto C., Lin R., et al.* Solving systems of Boolean multivariate equations with quantum annealing. Phys. Rev. Res., 2022, vol. 4, no. 1, paper 013096.
7. *Bennakhi A., Byrd G. T., and Franzon P.* Solving the B-SAT problem using quantum computing: Smaller is sometimes better. Entropy, 2024, vol. 26, no. 10, paper 875.
8. *Leont'ev V. K. and Tonoyan G. P.* Approximate solutions of systems of Boolean equations. Comput. Math. Math. Phys., 1993, vol. 33, no. 9, pp. 1221–1227.
9. *Leont'ev V. K. and Gordeev E. N.* On the number of solutions to a system of Boolean equations. Autom. Remote Control, 2021, vol. 82, no. 9, pp. 1581–1596.
10. *Gu J.* How to Solve Very Large-Scale Satisfiability (VLSS) Problems. Technical Report UCECETR-90-002, Calgary, University of Calgary, 1990.
11. *Gu J.* On optimizing a search problem. N. G. Burbakis (ed). Artificial Intelligence Methods and Applications, 1992, pp. 63–105.
12. *Gu J.* Global optimization for satisfiability (SAT) problem. IEEE Trans. Knowledge Data Engin., 1994, vol. 6, no. 3, pp. 361–381.
13. *Gu J., Gu Q., and Du D.* On optimizing the satisfiability (SAT) problem. J. Computer Sci. Technology, 1999, vol. 14, no. 1, pp. 1–17.
14. *Barotov D. N.* Target function without local minimum for systems of logical equations with a unique solution. Mathematics, 2022, vol. 10, no. 12:2097.
15. *Pakhomchik A. I., Voloshinov V. V., Vinokur V. M., and Lesovik G. B.* Converting of Boolean expression to linear equations, inequalities and QUBO penalties for cryptanalysis. Algorithms, 2022, vol. 15, no. 2:33.
16. *Burek E., Wronski M., Mank K., and Misztal M.* Algebraic attacks on block ciphers using quantum annealing. IEEE Trans. Emerging Topics in Computing, 2022, vol. 10, no. 2, pp. 678–689.

17. *Abdel-Gawad A. H., Atiya A. F., and Darwish N. M.* Solution of systems of Boolean equations via the integer domain. Inform. Sci., 2010, vol. 180, no. 2, pp. 288–300.
18. *Barotov D. N., Barotov R. N., Soloviev V., et al.* The development of suitable inequalities and their application to systems of logical equations. Mathematics, 2022, vol. 10, no. 11:1851.
19. *Faizullin R. T., Dulkeyt V. I., and Ogorodnikov Y. Y.* Gibridnyy metod poiska priblizhennogo resheniya zadachi 3-vypolnimost', assotsiirovannoy s zadachey faktorizatsii [Hybrid method for the approximate solution of the 3-satisfiability problem associated with the factorization problem]. Tr. Inst. Mat. Mekh., 2013, vol. 19, no. 2, pp. 285–294. (in Russian)
20. *Barotov D. N. and Barotov R. N.* Polilineynyye prodolzheniya nekotorykh diskretnykh funktsiy i algoritm ikh nakhozhdeniya [Polylinear continuations of some discrete functions and an algorithm for finding them]. Vychislitel'nye Metody i Programmirovanie, 2023, vol. 24, pp. 10–23. (in Russian)
21. *Barotov D. N. and Barotov R. N.* Konstruirovaniye gladkikh vypuklykh prodolzheniy bulevykh funktsiy [Construction of smooth convex extensions of Boolean functions]. Vestnik Rossiyskikh Universitetov. Matematika, 2024, vol. 29, no. 145, pp. 20–28. (in Russian)
22. *Barotov D. N.* Convex continuation of a Boolean function and its applications. J. Appl. Industr. Math., 2024, vol. 18, no. 1, pp. 1–9.
23. *Barotov D. N.* On the existence and properties of convex extensions of Boolean functions. Math. Notes, 2024, vol. 115, no. 4, pp. 489–505.
24. *Barotov D. N.* Vognutyye prodolzheniya bulevykh funktsiy i nekotoryye ikh svoystva i prilozheniya [Concave continuations of Boolean functions and some of their properties and applications]. Izvestiya Irkutskogo Gosuniversiteta. Ser. Matematika, 2024, vol. 49, pp. 105–123. (in Russian)
25. *Barotov D. N.* Convex continuations of some discrete functions. J. Appl. Industr. Math., 2024, vol. 18, no. 3, pp. 412–423.
26. *Barotov D. N. and Sudakov V. A.* O neravenstvakh mezhdu vypuklymi, vognutymi i polilineynymi prodolzheniyami bulevykh funktsiy [On inequalities between convex, concave, and multilinear continuations of Boolean functions]. Preprinty IPM im. M. V. Keldysha, 2024, no. 30, pp. 1–13. (in Russian)
27. *Ekeland I. and Temam R.* Convex Analysis and Variational Problems. Amsterdam, North-Holland, 1976. 402 p.
28. *Salomaa A.* On essential variables of functions, especially in the algebra of logic. Ann. Acad. Sci. Fenn. Ser. AI Math., 1963, no. 339, pp. 1–11.
29. *Jensen J. L. W. V.* Sur les fonctions convexes et les inegalites entre les valeurs moyennes. Acta Mathematica, 1906, vol. 30, no. 1, pp. 175–193. (in French)