ISSN 2686-9667. Вестник российских университетов. Математика

Том 29, № 145 2024

НАУЧНАЯ СТАТЬЯ

https://doi.org/10.20310/2686-9667-2024-29-145-20-28
УДК 519.85, 517.518.244

Конструирование гладких выпуклых продолжений булевых функций

Достонжон Нумонжонович БАРОТОВ[1] **, Рузибой Нумонжонович БАРОТОВ**[2]

[1] ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»
125167, Российская Федерация, г. Москва, пр-т Ленинградский, 49/2

[2] Худжандский государственный университет имени академика Б. Гафурова
735700, Республика Таджикистан, г. Худжанд, проезд Мавлонбекова, 1

Аннотация. Системы булевых уравнений широко используются в математике, компьютерных и прикладных науках. В связи с этим, с одной стороны, для таких систем разрабатываются новые методы и алгоритмы исследования, а с другой — совершенствуются существующие методы и алгоритмы решения таких систем. Один из методов заключается в том, что, во-первых, система булевых уравнений, заданная над кольцом булевых полиномов, трансформируется в систему уравнений над полем действительных чисел, а во-вторых, трансформированная система сводится либо к задаче численной минимизации соответствующей целевой функции, либо к задаче MILP или QUBO, либо к системе полиномиальных уравнений, решаемой на множестве целых чисел, либо к эквивалентной системе полиномиальных уравнений, решаемой символьными методами. Имеется много способов, позволяющих трансформировать систему булевых уравнений в задачу непрерывной минимизации, поскольку принципиальное отличие таких методов от «переборных» алгоритмов локального поиска — на каждой итерации алгоритма сдвиг по антиградиенту производится по всем переменным одновременно. Но одна из основных проблем, возникающая при применении этих способов, состоит в том, что минимизируемая целевая функция в искомой области может иметь множество локальных минимумов, что значительно усложняет их практическое использование. В работе строится неотрицательное выпуклое и непрерывно дифференцируемое продолжение произвольной булевой функции, которое применяется к решению произвольной системы булевых уравнений. Утверждается, что задача решения произвольной системы булевых уравнений может быть конструктивно сведена к задаче минимизации функции, любой локальный минимум которой в искомой области является глобальным минимумом.

Ключевые слова: глобальная оптимизация, выпуклая функция, булева функция, продолжение булевой функции, локальный минимум

Для цитирования: *Баротов Д.Н., Баротов Р.Н.* Конструирование гладких выпуклых продолжений булевых функций // Вестник российских университетов. Математика. 2024. Т. 29. № 145. С. 20–28. https://doi.org/10.20310/2686-9667-2024-29-145-20-28

SCIENTIFIC ARTICLE

https://doi.org/10.20310/2686-9667-2024-29-145-20-28

Construction of smooth convex extensions of Boolean functions

Dostonjon N. BAROTOV[1] **, Ruziboy N. BAROTOV**[2]

[1] Financial University under the Government of the Russian Federation
49/2 Leningradsky Prospekt, Moscow 125167, Russian Federation

[2] Khujand State University named after academician Bobojon Gafurov
1 Mavlonbekova, Khujand 735700, Republic of Tajikistan

Abstract. Systems of Boolean equations are widely used in mathematics, computer science, and applied sciences. In this regard, on the one hand, new research methods and algorithms are being developed for such systems, and on the other hand, existing methods and algorithms for solving such systems are being improved. One of these methods is that, firstly, the system of Boolean equations given over the ring of Boolean polynomials is transformed into a system of equations over the field of real numbers, and secondly, the transformed system is reduced either to the problem of numerical minimization of the corresponding objective function, to a MILP or QUBO problem, to a system of polynomial equations solved on the set of integers, or to an equivalent system of polynomial equations solved by symbolic methods. There are many ways to transform a system of Boolean equations into a continuous minimization problem, since the fundamental difference between such methods and "brute force" local search algorithms is that at each iteration of the algorithm, the shift along the antigradient is performed on all variables simultaneously. But one of the main problems that arise when applying these methods is that the objective function to be minimized in the desired area can have many local minima, which greatly complicates their practical use. In this paper, a non-negative convex and continuously differentiable extension of any Boolean function is constructed, which is applied to solving an arbitrary system of Boolean equations. It is argued that the problem of solving an arbitrary system of Boolean equations can be constructively reduced to the problem of minimizing a function, any local minimum of which in the desired domain is a global minimum.

Keywords: global optimization, convex function, Boolean function, extension of a Boolean function, local minimum

Mathematics Subject Classification: 65K05, 90C25, 46N10.

For citation: Barotov D.N., Barotov R.N. Construction of smooth convex extensions of Boolean functions. *Vestnik rossiyskikh universitetov. Matematika = Russian Universities Reports. Mathematics*, **29**:145 (2024), 20–28. https://doi.org/10.20310/2686-9667-2024-29-145-20-28
(In Russian, Abstr. in Engl.)

Введение

На протяжении многих десятилетий в истории цифровой науки булевы переменные были основными переменными, используемыми в большинстве компьютерных операций. Встречается много основных задач, связанных с булевыми переменными, а некоторые задачи, несмотря на зрелость области, не имеют удовлетворительных методов решения. Среди них проблема решения булевых и систем булевых уравнений [1]. Эта задача имеет множество приложений, таких как синтез, моделирование и тестирование цифровых сетей и систем СБИС, кодирование выходных данных и назначение состояний конечных автоматов, временной анализ и генерация тестов с задержкой-сбоем для комбинационных схем, автоматическая генерация тестовых шаблонов, определение начального состояния в схемах, содержащих петли обратной связи. В области криптографии булевы уравнения находят применение при анализе и взломе блочных шифров, поскольку их можно свести к проблеме решения крупномасштабной системы булевых уравнений [1–3]. И в настоящем времени теория булевых функций — увлекательная область исследований в области дискретной математики с приложениями к криптографии и теории кодирования [4]. Булевы функции с высокой нелинейностью могут быть использованы для внесения путаницы в алгоритмы блочного шифрования [4, 5]. В связи с этим развивается множество новых направлений исследования и алгоритмов решения систем булевых уравнений. Одно из направлений заключается в том, что, во-первых, система булевых уравнений, заданная над кольцом булевых полиномов, преобразуется в систему уравнений над полем действительных чисел, а во-вторых, преобразованная система сводится либо к задаче численной минимизации соответствующей целевой функции [6–8], либо к задаче MILP или QUBO [9], либо к системе полиномиальных уравнений, решаемой на множестве целых чисел [1], либо к эквивалентной системе полиномиальных уравнений, решаемой символьными методами [10].

Имеется много способов, позволяющих преобразовать систему булевых уравнений в задачу непрерывной минимизации, поскольку принципиальное отличие таких методов от «переборных» алгоритмов локального поиска — на каждой итерации алгоритма сдвиг по антиградиенту производится по всем переменным одновременно [2,3,6–8,11–14]. Но одна из основных проблем, возникающая при применении этих способов, заключается в том, что минимизируемая целевая функция в искомой области может иметь множество локальных минимумов, что значительно усложняет их практическое использование [2, 3, 6–8, 11, 12]. По теореме Д. Н. Баротова, полилинейное продолжение булевой функции играет важную роль в том числе и для уменьшения числа локальных минимумов целевой функции [3, 11]. Недавно в работе [11] были найдены явные формы полилинейных продолжений для произвольных функций, определенных на множестве вершин n-мерного единичного куба, произвольного куба и параллелепипеда, и в каждом конкретном случае была доказана единственность соответствующего полилинейного продолжения.

В данной работе конструируется неотрицательное выпуклое и непрерывно дифференцируемое продолжение любой булевой функции и вследствие утверждается, что задача решения произвольной системы булевых уравнений может быть конструктивно сведена к задаче минимизации функции, любой локальный минимум которой в искомой области является глобальным минимумом.

1. Основные понятия

Пусть $\mathbf{B}^n = \{(b_1, b_2, \ldots, b_n) : b_1, b_2, \ldots, b_n \in \{0,1\}\}$ — множество всевозможных двоичных слов (булевых векторов) длины n, $\mathbf{K}^n = \{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in [0,1]\}$ — n-мерный куб, натянутый на булевые векторы длины n, $\mathrm{int}(\mathbf{K}^n) = \{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in (0,1)\}$ — внутренность куба $\mathbf{K}^n$, $\mathbf{FK}^n_{(b_1,b_2,\ldots,b_n)} = \{(x_1, x_2, \ldots, x_n) \in \mathbf{K}^n : (2b_1-1)x_1 + (2b_2-1)x_2 + \ldots + (2b_n-1)x_n \le b_1 + b_2 + \ldots + b_n - 1\}$ — фрагмент куба $\mathbf{K}^n$, противолежащий вершине $(b_1, b_2, \ldots, b_n) \in \mathbf{B}^n$.

О п р е д е л е н и е 1.1. Функцию $f : \mathbf{K}^n \to \mathbf{R}$ назовем неотрицательной выпуклой функцией на $\mathbf{K}^n$, если для любых $x, y \in \mathbf{K}^n$ и любого $\alpha \in [0,1]$ выполняется

$$0 \le f(\alpha \cdot x + (1-\alpha) \cdot y) \le \alpha \cdot f(x) + (1-\alpha) \cdot f(y).$$

О п р е д е л е н и е 1.2. Функцию $p_C : \mathbf{K}^n \to \mathbf{R}$ назовем неотрицательным выпуклым продолжением на $\mathbf{K}^n$ булевой функции $p : \mathbf{B}^n \to \{0,1\}$, если выполнены два следующих условия:

a) функция p_C является выпуклой и неотрицательной на $\mathbf{K}^n$,

b) $p_C(b_1, b_2, \ldots, b_n) = p(b_1, b_2, \ldots, b_n) \quad \forall (b_1, b_2, \ldots, b_n) \in \mathbf{B}^n$.

2. Основные результаты

Лемма 2.1. *Для булевой функции* $K_{(b_1,b_2,\ldots,b_n)}$, *заданной формулой*

$$K_{(b_1,b_2,\ldots,b_n)}(x_1, x_2, \ldots, x_n) = x_1^{b_1} \wedge x_2^{b_2} \wedge \ldots \wedge x_n^{b_n},$$

существует выпуклое неотрицательное продолжение $f_{(b_1,b_2,\ldots,b_n)}$ *на* $\mathbf{K}^n$.

Д о к а з а т е л ь с т в о. Для конструирования искомого продолжения заданной булевой функции сначала покажем, что если $f_{(b_1,b_2,\ldots,b_n)}$ — неотрицательное выпуклое продолжение на $\mathbf{K}^n$ функции $K_{(b_1,b_2,\ldots,b_n)}$, то для любого вектора $(x_1^*, x_2^*, \ldots, x_n^*) \in \mathbf{FK}^n_{(b_1,b_2,\ldots,b_n)}$ выполнено $f_{(b_1,b_2,\ldots,b_n)}(x_1^*, x_2^*, \ldots, x_n^*) = 0$.

Включение $(x_1^*, x_2^*, \ldots, x_n^*) \in \mathbf{FK}^n_{(b_1,b_2,\ldots,b_n)}$ означает, что

$$(x_1^*, x_2^*, \ldots, x_n^*) = \sum_{(a_1,a_2,\ldots,a_n) \in \mathbf{B}^n \setminus \{(b_1,b_2,\ldots,b_n)\}} \lambda^*_{(a_1,a_2,\ldots,a_n)} \cdot (a_1, a_2, \ldots, a_n),$$

где $\lambda^*_{(a_1,a_2,\ldots,a_n)} \ge 0$ и $\sum\limits_{(a_1,a_2,\ldots,a_n) \in \mathbf{B}^n \setminus \{(b_1,b_2,\ldots,b_n)\}} \lambda^*_{(a_1,a_2,\ldots,a_n)} = 1$. Теперь, с одной стороны, $(x_1^*, x_2^*, \ldots, x_n^*) \in \mathbf{K}^n$ и функция $f_{(b_1,b_2,\ldots,b_n)}(x_1, x_2, \ldots, x_n)$ неотрицательна на $\mathbf{K}^n$ и, следовательно, $0 \le f_{(b_1,b_2,\ldots,b_n)}(x_1^*, x_2^*, \ldots, x_n^*)$, с другой стороны, в силу неравенства Йенсена [15]

$$\begin{aligned} f_{(b_1,b_2,\ldots,b_n)}(x_1^*, x_2^*, \ldots, x_n^*) &= f_{(b_1,b_2,\ldots,b_n)}\left(\sum_{(a_1,a_2,\ldots,a_n) \in \mathbf{B}^n \setminus \{(b_1,b_2,\ldots,b_n)\}} \lambda^*_{(a_1,a_2,\ldots,a_n)} \cdot (a_1, a_2, \ldots, a_n) \right) \\ &\le \sum_{(a_1,a_2,\ldots,a_n) \in \mathbf{B}^n \setminus \{(b_1,b_2,\ldots,b_n)\}} \lambda^*_{(a_1,a_2,\ldots,a_n)} \cdot f_{(b_1,b_2,\ldots,b_n)}(a_1, a_2, \ldots, a_n) \\ &= \sum_{(a_1,a_2,\ldots,a_n) \in \mathbf{B}^n \setminus \{(b_1,b_2,\ldots,b_n)\}} \lambda^*_{(a_1,a_2,\ldots,a_n)} \cdot 0 = 0. \end{aligned}$$

Из двух полученных неравенств $0 \le f_{(b_1,b_2,\dots,b_n)}(x_1^*, x_2^*, \dots, x_n^*) \le 0$ следует, что

$$f_{(b_1,b_2,\dots,b_n)}(x_1^*, x_2^*, \dots, x_n^*) = 0 \quad \forall (x_1^*, x_2^*, \dots, x_n^*) \in \mathbf{FK}^n_{(b_1,b_2,\dots,b_n)}. \tag{2.1}$$

Теперь, пусть $(x_1^*, x_2^*, \dots, x_n^*) \in \mathbf{K}^n \setminus \mathbf{FK}^n_{(b_1,b_2,\dots,b_n)}$. В этой точке значение функции $f_{(b_1,b_2,\dots,b_n)}$ определим формулой

$$f_{(b_1,b_2,\dots,b_n)}(x_1^*, x_2^*, \dots, x_n^*) = \Big(1 + \sum_{k=1}^{n} \big((2b_k - 1)x_k^* - b_k\big)\Big)^2. \tag{2.2}$$

Заметим, что

$$f_{(b_1,b_2,\dots,b_n)}(b_1, b_2, \dots, b_n) = \Big(1 + \sum_{k=1}^{n} \big((2b_k - 1)b_k - b_k\big)\Big)^2 = \Big(1 - \sum_{k=1}^{n} 2b_k(1 - b_k)\Big)^2 = 1. \tag{2.3}$$

Таким образом, из равенств (2.1)–(2.3) следует, что сконструированная выше функция $f_{(b_1,b_2,\dots,b_n)}$ неотрицательна и

$$\begin{aligned} f_{(b_1,b_2,\dots,b_n)}(a_1, a_2, \dots, a_n) &= \begin{cases} 0, & \text{если } (a_1, a_2, \dots, a_n) \in \mathbf{B}^n \setminus \{(b_1, b_2, \dots, b_n)\}, \\ 1, & \text{если } (a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n), \end{cases} \\ &= K_{(b_1,b_2,\dots,b_n)}(a_1, a_2, \dots, a_n). \end{aligned}$$

Чтобы завершить доказательство, остается показать, что функция $f_{(b_1,b_2,\dots,b_n)}$ является выпуклой на $\mathbf{K}^n$. Объединив (2.1), (2.2), получим

$$f_{(b_1,b_2,\dots,b_n)}(x_1, x_2, \dots, x_n) = \begin{cases} 0, & \text{если } 1 + \sum\limits_{k=1}^{n} \big((2b_k - 1)x_k - b_k\big) \le 0, \\ \Big(1 + \sum\limits_{k=1}^{n} \big((2b_k - 1)x_k - b_k\big)\Big)^2, & \text{если } 1 + \sum\limits_{k=1}^{n} \big((2b_k - 1)x_k - b_k\big) \ge 0. \end{cases}$$

Правая часть этого равенства может быть записана в следующем виде

$$\frac{1}{4}\left[\Big(1 + \sum_{k=1}^{n} \big((2b_k - 1)x_k - b_k\big)\Big) + \Big|1 + \sum_{k=1}^{n} \big((2b_k - 1)x_k - b_k\big)\Big|\right]^2. \tag{2.4}$$

Используя (2.4), для любых $x, y \in \mathbf{K}^n$ и $\alpha \in [0, 1]$ получаем

$$\begin{aligned} f_{(b_1,b_2,\dots,b_n)}(\alpha x + (1 - \alpha)y) &= \frac{1}{4}\Bigg[\sum_{k=1}^{n} \big((2b_k - 1)(\alpha x_k + (1 - \alpha)y_k) - b_k\big) + 1 \\ &\quad + \Big|\sum_{k=1}^{n} ((2b_k - 1)(\alpha x_k + (1 - \alpha)y_k) - b_k) + 1\Big|\Bigg]^2 \\ = \frac{1}{4}\Bigg[&\alpha\Big(\sum_{k=1}^{n} ((2b_k - 1)x_k - b_k) + 1\Big) + (1 - \alpha)\Big(\sum_{k=1}^{n}((2b_k - 1)y_k - b_k) + 1\Big) \\ + \Big|&\alpha\Big(\sum_{k=1}^{n} ((2b_k - 1)x_k - b_k) + 1\Big) + (1 - \alpha)\Big(\sum_{k=1}^{n}((2b_k - 1) \cdot y_k - b_k) + 1\Big)\Big|\Bigg]^2 \end{aligned}$$

$$
\begin{aligned}
&\le \frac{1}{4}\Bigg[\alpha\Big(\sum_{k=1}^{n}\big((2b_k-1)x_k-b_k\big)+1\Big)+(1-\alpha)\Big(\sum_{k=1}^{n}((2b_k-1)y_k-b_k)+1\Big)\\
&+\alpha\Big|\sum_{k=1}^{n}\big((2b_k-1)x_k-b_k\big)+1\Big|+(1-\alpha)\Big|\sum_{k=1}^{n}\big((2b_k-1)y_k-b_k\big)+1\Big|\Bigg]^2\\
&=\frac{1}{4}\Bigg[\alpha\Big\{\sum_{k=1}^{n}\big((2b_k-1)x_k-b_k\big)+1+\Big|\sum_{k=1}^{n}\big((2b_k-1)x_k-b_k\big)+1\Big|\Big\}\\
&+(1-\alpha)\Big\{\sum_{k=1}^{n}\big((2b_k-1)y_k-b_k\big)+1+\Big|\sum_{k=1}^{n}\big((2b_k-1)y_k-b_k\big)+1\Big|\Big\}\Bigg]^2\\
&\le\frac{1}{4}\Bigg[\alpha\Big\{\sum_{k=1}^{n}\big((2b_k-1)x_k-b_k\big)+1+\Big|\sum_{k=1}^{n}\big((2b_k-1)x_k-b_k\big)+1\Big|\Big\}^2\\
&+(1-\alpha)\Big\{\sum_{k=1}^{n}\big((2b_k-1)y_k-b_k\big)+1+\Big|\sum_{k=1}^{n}\big((2b_k-1)y_k-b_k\big)+1\Big|\Big\}^2\Bigg]\\
&=\alpha f_{(b_1,b_2,\dots,b_n)}(x)+(1-\alpha)f_{(b_1,b_2,\dots,b_n)}(y).
\end{aligned}
$$

Таким образом, функция $f_{(b_1,b_2,\dots,b_n)}$ является выпуклой на $\mathbf{K}^n$. □

З а м е ч а н и е 2.1. Неотрицательное выпуклое продолжение на $\mathbf{K}^n$ булевой функции $K_{(b_1,b_2,\dots,b_n)}$ является не единственным. Например, если $f_{(b_1,b_2,\dots,b_n)}$ является таким продолжением, то и функция, имеющая значения $\big(f_{(b_1,b_2,\dots,b_n)}(x_1,x_2,\dots,x_n)\big)^2$, также будет неотрицательным выпуклым продолжением на $\mathbf{K}^n$ функции $K_{(b_1,b_2,\dots,b_n)}$.

Теорема 2.1. *Для произвольной булевой функции $p:\mathbf{B}^n\to\{0,1\}$ существует выпуклое неотрицательное продолжение p_C на $\mathbf{K}^n$.*

Д о к а з а т е л ь с т в о. Пусть задана булева функция $p:\mathbf{B}^n\to\{0,1\}$. Используя подходы, предложенные в [11, теорема 2], зададим функцию $p_C:\mathbf{K}^n\to\mathbf{R}$ формулой

$$
p_C(x_1,x_2,\dots,x_n)=\sum_{(b_1,b_2,\dots,b_n)\in\mathbf{B}^n}p(b_1,b_2,\dots,b_n)\cdot f_{(b_1,b_2,\dots,b_n)}(x_1,x_2,\dots,x_n),\tag{2.5}
$$

где функция $f_{(b_1,b_2,\dots,b_n)}$, являющаяся выпуклым неотрицательным продолжением булевой функции $K_{(b_1,b_2,\dots,b_n)}$, определена в лемме 2.1. Докажем, что функция (2.5) является требуемым продолжением булевой функции p.

Сначала заметим, что в силу определения функция p_C выпукла на множестве $\mathbf{K}^n$, так как является суммой выпуклых функций.

Остается проверить, что для любого $(a_1,a_2,\dots,a_n)\in\mathbf{B}^n$ выполнено $p_C(a_1,a_2,\dots,a_n)=p(a_1,a_2,\dots,a_n)$. Действительно, в силу леммы 2.1 имеем:

$$
\begin{aligned}
p_C(a_1,a_2,\dots,a_n)&=\sum_{(b_1,b_2,\dots,b_n)=(a_1,a_2,\dots,a_n)}p(b_1,b_2,\dots,b_n)\cdot f_{(b_1,b_2,\dots,b_n)}(a_1,a_2,\dots,a_n)\\
&+\sum_{(b_1,b_2,\dots,b_n)\in\mathbf{B}^n\setminus(a_1,a_2,\dots,a_n)}p(b_1,b_2,\dots,b_n)\cdot f_{(b_1,b_2,\dots,b_n)}(a_1,a_2,\dots,a_n)\\
&=p(a_1,a_2,\dots,a_n)\cdot f_{(a_1,a_2,\dots,a_n)}(a_1,a_2,\dots,a_n)\\
&+\sum_{(b_1,b_2,\dots,b_n)\in\mathbf{B}^n\setminus(a_1,a_2,\dots,a_n)}p(b_1,b_2,\dots,b_n)\cdot 0=p(a_1,a_2,\dots,a_n).
\end{aligned}
$$

Итак, доказано, что функция (2.5) является выпуклым неотрицательным продолжением на $\mathbf{K}^n$ булевой функции p. □

З а м е ч а н и е 2.2. Если для булевой функции p выполнено $p(x_1, x_2, \ldots, x_n) \equiv 0$, то ее неотрицательное выпуклое продолжение p_C на $\mathbf{K}^n$ определяется единственным образом, причем в этом случае $p_C(x_1, x_2, \ldots, x_n) = 0 \ \ \forall (x_1, x_2, \ldots, x_n) \in \mathbf{K}^n$. Действительно, для $(x_1, x_2, \ldots, x_n) \in \mathbf{K}^n$ выполнено

$$
\begin{aligned}
0 \le p_C(x_1, x_2, \ldots, x_n) &= p_C((1-x_1)\cdot 0 + x_1 \cdot 1, x_2, \ldots, x_n) \\
&= p_C((1-x_1)\cdot 0 + x_1 \cdot 1, (1-x_1)\cdot x_2 + x_1 \cdot x_2, \ldots, (1-x_1)\cdot x_n + x_1 \cdot x_n) \\
&\le (1-x_1)\cdot p_C(0, x_2, \ldots, x_n) + x_1 \cdot p_C(1, x_2, \ldots, x_n) \\
&\le \ldots \le \sum_{(b_1,b_2,\ldots,b_n)\in \mathbf{B}^n} p_C(b_1, b_2, \ldots, b_n) \cdot \prod_{k=1}^{n} ((2b_k - 1)x_k + 1 - b_k) \\
= \sum_{(b_1,b_2,\ldots,b_n)\in \mathbf{B}^n} p(b_1, b_2, \ldots, b_n) \cdot \prod_{k=1}^{n} ((2b_k - 1)x_k + 1 - b_k) &= \sum_{(b_1,b_2,\ldots,b_n)\in \mathbf{B}^n} 0 \cdot \prod_{k=1}^{n} ((2b_k - 1)x_k + 1 - b_k) = 0.
\end{aligned}
$$

З а м е ч а н и е 2.3. Если для булевой функции p выполнено $p(x_1, x_2, \ldots, x_n) \not\equiv 0$, то ее неотрицательное выпуклое продолжение p_C на $\mathbf{K}^n$ не является единственным. Это прямо следует из неединственности функции $f_{(b_1,b_2,\ldots,b_n)}$, через которую формулой (2.5) определяется функция p_C (см. замечание 2.1).

3. Применение выпуклого продолжения булевой функции к решению системы булевых уравнений

Рассмотрим систему булевых уравнений

$$
p_1(x_1, x_2, \ldots, x_n) = 0, \ \cdots, \ p_m(x_1, x_2, \ldots, x_n) = 0. \tag{3.1}
$$

Трансформируем эту систему в соответствующую систему выпуклых уравнений

$$
p_{C1}(x_1, x_2, \ldots, x_n) = 0, \ \cdots, \ p_{Cm}(x_1, x_2, \ldots, x_n) = 0, \tag{3.2}
$$

где функция p_{Ci} — выпуклое продолжение булевой функции p_i, $i = \overline{1, m}$, т. е., как показано при доказательстве теоремы 2.1, может быть определена формулой

$$
p_{Ci}(x_1, x_2, \ldots, x_n) = \sum_{(b_1,b_2,\ldots,b_n)\in \mathbf{B}^n} p_i(b_1, b_2, \ldots, b_n) \cdot f_{(b_1,b_2,\ldots,b_n)}(x_1, x_2, \ldots, x_n).
$$

Задача решения системы (3.2), очевидно, сводится к задаче минимизации функции $\overline{p}_C$, определяемой соотношением

$$
\overline{p}_C(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} p_{Ci}(x_1, x_2, \ldots, x_n).
$$

Перечислим некоторые свойства функции $\overline{p}_C$, полезные при решении задачи минимизации (в частности, с точки зрения уменьшения количества локальных минимумов).

С в о й с т в о 3.1. На множестве $\mathbf{K}^n$ функция $\overline{p}_C$ выпуклая и непрерывно дифференцируемая.

С в о й с т в о 3.2. На множестве $\mathbf{K}^n$ любой локальный минимум функции $\overline{p}_C$ является также и глобальным минимумом.

С в о й с т в о 3.3. Если вектор $(s_1, s_2, \ldots, s_n) \in \mathbf{B}^n$ является решением системы (3.1), то он будет являться решением системы (3.2) и $\overline{p}_C(s_1, s_2, \ldots, s_n) = 0$.

С в о й с т в о 3.4. Вектор $(r_1, r_2, \ldots, r_n) \in \mathbf{K}^n$ будет решением системы (3.2) в том и только в том случае, когда $\overline{p}_C(r_1, r_2, \ldots, r_n) = 0$.

Справедливость свойств 3.1–3.4 следует из определения функции $\overline{p}_C$.

Авторы выражают искреннюю благодарность рецензенту за полезные замечания и нахождение ряда недостатков, исправление которых помогло улучшить содержание статьи.

References

[1] A. H. Abdel-Gawad, A. F. Atiya, N. M. Darwish, "Solution of systems of Boolean equations via the integer domain", *Information Sciences*, **180**:2 (2010), 288–300.

[2] D. N. Barotov, R. N. Barotov, "Polylinear transformation method for solving systems of logical equations", *Mathematics*, **10**:6 (2022), 918.

[3] D. N. Barotov, "Target function without local minimum for systems of logical equations with a unique solution", *Mathematics*, **10**:12 (2022), 2097.

[4] J. A. Armario, "Boolean functions and permanents of Sylvester Hadamard matrices", *Mathematics*, **9**:2 (2021), 177.

[5] L. G. Valiant, "The complexity of computing the permanent", *Theoretical Computer Science*, **8**:2 (1979), 189–201.

[6] Р. Т. Файзуллин, В. И. Дулькейт, Ю. Ю. Огородников, "Гибридный метод поиска приближенного решения задачи 3-выполнимость, ассоциированной с задачей факторизации", Тр. ИММ УрО РАН, **19**, 2013, 285–294. [R. T. Faizullin, V. I. Dul'keit, Yu. Yu. Ogorodnikov, "Hybrid method for the approximate solution of the 3-satisfiability problem associated with the factorization problem", *Trudy Inst. Mat. i Mekh. UrO RAN*, **19**:2 (2013), 285–294 (In Russian)].

[7] J. Gu, "Global optimization for satisfiability (SAT) problem", *IEEE Transactions on Knowledge and DataEngineering*, **6**:3 (1994), 361–381.

[8] J. Gu, Q. Gu, D. Du, "On optimizing the satisfiability (SAT) problem", *Journal of Computer Science and Technology*, **14**:1 (1999), 1–17.

[9] A. I. Pakhomchik, V. V. Voloshinov, V. M. Vinokur, G. B. Lesovik, "Converting of Boolean expression to linear equations, inequalities and QUBO penalties for cryptanalysis", *Algorithms*, **15**:2 (2022), 33.

[10] D. N. Barotov, R. N. Barotov, V. Soloviev, V. Feklin, D. Muzafarov, T. Ergashboev, Kh. Egamov, "The development of suitable inequalities and their application to systems of logical equations", *Mathematics*, **10**:11 (2022), 1851.

[11] D. N. Barotov, R. N. Barotov, "Polylinear continuations of some discrete functions and an algorithm for finding them", *Numerical Methods and Programming (Vychislitel'nye Metody i Programmirovanie)*, **24**:1 (2023), 10–23.

[12] D. N. Barotov, A. Osipov, S. Korchagin, E. Pleshakova, D. Muzafarov, R. Barotov, D. Serdechnyy, "Transformation method for solving system of Boolean algebraic equations", *Mathematics*, **9**:24 (2021), 3299.

[13] G. Owen, "Multilinear extensions of games", *Management Science*, **18**:(5-part-2) (1972), 64–79.

[14] D. M. Wittmann, J. Krumsiek, J. Saez-Rodriguez, D. A. Lauffenburger, S. Klamt, F. J. Theis, "Transforming Boolean models to continuous models: methodology and application to T-cell receptor signaling", *BMC Systems Biology*, **3** (2009), 98(2009).

[15] J. L. W. V. Jensen, "Sur les fonctions convexes et les inegalites entre les valeurs moyennes", *Acta Mathematica*, **30** (1906), 175–193.

Информация об авторах

Баротов Достонжон Нумонжонович, старший преподаватель департамента анализа данных и машинного обучения, Финансовый университет при Правительстве РФ, г. Москва, Российская Федерация. E-mail: DNBarotov@fa.ru
ORCID: https://orcid.org/0000-0001-5047-7710

Баротов Рузибой Нумонжонович, докторант, кафедра математического анализа имени профессора А. Мухсинова, Худжандский государственный университет имени академика Б. Гафурова, г. Худжанд, Республика Таджикистан. E-mail: ruzmet.tj@mail.ru
ORCID: https://orcid.org/0000-0003-3729-6143

Конфликт интересов отсутствует.

Для контактов:
Баротов Достонжон Нумонжонович
E-mail: DNBarotov@fa.ru

Поступила в редакцию 09.07.2023 г.
Поступила после рецензирования 13.02.2024 г.
Принята к публикации 11.03.2024 г.

Information about the authors

Dostonjon N. Barotov, Senior Lecturer, Data Analysis and Machine Learning Department, Financial University under the Government of the Russian Federation, Moscow, Russian Federation. E-mail: DNBarotov@fa.ru
ORCID: https://orcid.org/0000-0001-5047-7710

Ruziboy N. Barotov, Doctoral Student, Mathematical Analysis named after Professor A. Mukhsinov Department, Khujand State University named after academician Bobojon Gafurov, Khujand, Republic of Tajikistan. E-mail: ruzmet.tj@mail.ru
ORCID: https://orcid.org/0000-0003-3729-6143

There is no conflict of interests.

Corresponding author:
Dostonjon N. Barotov
E-mail: DNBarotov@fa.ru

Received 09.07.2023
Reviewed 13.02.2024
Accepted for press 11.03.2024