

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 26. Выпуск 3.

УДК 519.716.322, 517.518.244, 512.563

DOI 10.22405/2226-8383-2025-26-3-58-70

**О порядке гладкости максимального выпуклого продолжения
булевой функции**

Д. Н. Баротов, Р. Н. Баротов

Баротов Достонжон Нумонжонович — Финансовый университет при Правительстве Российской Федерации (г. Москва).

e-mail: DNBarotov@fa.ru

Баротов Рузбой Нумонжонович — Худжандский государственный университет имени академика Б. Гафурова (г. Худжанд).

e-mail: ruzmet.tj@mail.ru

Аннотация

Данная статья посвящена установлению порядка гладкости $f_{NR}(x_1, x_2, \dots, x_n)$ — наибольшего выпуклого продолжения на $[0, 1]^n$ любой булевой функции $f_B(x_1, x_2, \dots, x_n)$. В результате исследования для каждой булевой функции $f_B(x_1, x_2, \dots, x_n)$ установлен порядок дифференцируемости $f_{NR}(x_1, x_2, \dots, x_n)$ — соответствующего ей наибольшего выпуклого продолжения на $[0, 1]^n$, а именно, во-первых, с обеих сторон оценено наибольшее выпуклое продолжение $f_{NR}(x_1, x_2, \dots, x_n)$ так, что из чего следует непрерывность $f_{NR}(x_1, x_2, \dots, x_n)$ на $[0, 1]^n$ для любого натурального n , а во-вторых, доказано, что если число существенных переменных булевой функции $f_B(x_1, x_2, \dots, x_n)$ меньше двух, то на $[0, 1]^n$ наибольшее выпуклое продолжение $f_{NR}(x_1, x_2, \dots, x_n)$ бесконечно дифференцируемо, а если не меньше двух, то на $[0, 1]^n$ наибольшее выпуклое продолжение $f_{NR}(x_1, x_2, \dots, x_n)$ не является дифференцируемым, т. е. является лишь непрерывным.

Ключевые слова: выпуклое продолжение булевой функции, булева функция, выпуклая функция, глобальная оптимизация, локальный экстремум.

Библиография: 32 названия.

Для цитирования:

Баротов, Д. Н., Баротов, Р. Н. О порядке гладкости максимального выпуклого продолжения булевой функции // Чебышевский сборник, 2025, т. 26, вып. 3, с. 58–70.

CHEBYSHEVSKII SBORNIK
Vol. 26. No. 3.

UDC 519.716.322, 517.518.244, 512.563

DOI 10.22405/2226-8383-2025-26-3-58-70

**On the order of smoothness of the maximal convex continuation of
a Boolean function**

D. N. Barotov, R. N. Barotov

Barotov Dostonjon Numonjonovich — Financial University under the Government of the Russian Federation (Moscow).

e-mail: DNBarotov@fa.ru

Barotov Ruziboy Numonjonovich — Khujand state university named after academician Bobojon Gafurov (Khujand).

e-mail: ruzmet.tj@mail.ru

Abstract

This paper is devoted to establishing the order of smoothness of $f_{NR}(x_1, x_2, \dots, x_n)$ — the largest convex continuation to $[0, 1]^n$ of any Boolean function $f_B(x_1, x_2, \dots, x_n)$. As a result of the study, for each Boolean function $f_B(x_1, x_2, \dots, x_n)$, the order of differentiability of $f_{NR}(x_1, x_2, \dots, x_n)$ — the corresponding greatest convex continuation to $[0, 1]^n$ — was established, namely, firstly, the greatest convex continuation $f_{NR}(x_1, x_2, \dots, x_n)$ was estimated from both sides so that, which implies the continuity of $f_{NR}(x_1, x_2, \dots, x_n)$ on $[0, 1]^n$ for any natural n , and secondly, it was proved that if the number of essential variables of the Boolean function $f_B(x_1, x_2, \dots, x_n)$ is less than two, then on $[0, 1]^n$ the greatest convex continuation $f_{NR}(x_1, x_2, \dots, x_n)$ is infinite differentiable, and if there are at least two, then on $[0, 1]^n$ the largest convex continuation $f_{NR}(x_1, x_2, \dots, x_n)$ is not differentiable, i.e. it is only continuous.

Keywords: convex continuation of a Boolean function, Boolean function, convex function, global optimization, local extremum.

Bibliography: 32 titles.

For citation:

Barotov, D. N., Barotov, R. N. 2025, “On the order of smoothness of the maximal convex continuation of a Boolean function”, *Chebyshevskii sbornik*, vol. 26, no. 3, pp. 58–70.

1. Введение

Системы булевых уравнений широко используются в математике, компьютерных и прикладных науках. Решение системы булевых уравнений проникает во многие области современной науки, такие как логическое проектирование, биология, грамматика, химия, право, медицина, спектроскопия и теория графов [1, 2]. Многие важные задачи исследования операций можно свести к задаче решения системы булевых уравнений. Ярким примером является задача коалиционной игры n агентов с отношением доминирования между различными стратегиями [3]. Решения булевых уравнений также служат важным инструментом при обработке псевдобулевых уравнений, неравенств и связанных с ними задач целочисленного линейного программирования [3]. В последние годы еще одной важной и перспективной областью, в которой применяется решение системы булевых уравнений, является алгебраический криптоанализ, особенно применяется при анализе и атаках на блочные шифры, поскольку их можно свести к задаче решения крупномасштабной системы булевых уравнений [5, 6, 7, 8, 9, 4, 2].

Одно из первых успешных применений решения системы булевых уравнений в области криптографии было продемонстрировано в [6]. В связи с этим, с одной стороны, совершенствуются существующие методы и алгоритмы, с другой стороны, разрабатывается и адаптируется множество новых направлений исследования и алгоритмов решения систем булевых уравнений [5, 7, 8, 9, 10]. Одним из таких направлений исследования является преобразование (трансформация) системы булевых уравнений в систему уравнений над полем действительных чисел, поскольку в этой области известно множество методов и алгоритмов решения систем. Суть этого направления состоит в том, что система булевых уравнений преобразуется в систему уравнений над полем действительных чисел и решение ищется на множестве действительных чисел [11, 12, 13]. В свою очередь, преобразованная система может быть сведена либо к задаче численной оптимизации, что позволяет применять, анализировать и комбинировать такие методы, как алгоритм наискорейшего спуска, метод Ньютона и алгоритм координатного спуска и аналогичные методы вычислительной математики [14, 15, 16], либо к задаче MILP или QUBO, решаемой классическими алгоритмами дискретной оптимизации или квантовыми алгоритмами [17, 18], либо к системе полиномиальных уравнений, решаемой на множестве целых чисел [19], либо к эквивалентной системе полиномиальных уравнений, решаемой и анализируемой символьными методами [20, 21, 22, 4].

Имеется множество способов преобразования системы булевых уравнений к задаче непрерывной оптимизации, поскольку принципиальное отличие таких методов от “переборных” алгоритмов локального поиска состоит в том, что на каждой итерации алгоритма сдвиг по градиенту (антиградиенту) производится по всем переменным одновременно [23, 14, 15]. Но одна из основных проблем, возникающих при применении этих методов, заключается в том, что оптимизируемая целевая функция в искомой области может иметь множество локальных экстремумов, что существенно усложняет их практическое использование [26, 25, 24]. В [25, 24] аргументировано, что при решении системы булевых уравнений методом численной оптимизации полилинейное продолжение булевой функции также играет важную роль, в том числе в уменьшении числа локальных экстремумов соответствующей целевой функции. По этой тематике в [24] найдены явные формы полилинейных продолжений произвольных дискретных функций, заданных на множестве вершин n -мерного единичного куба, произвольного куба и параллелепипеда, и в каждом конкретном случае доказана единственность соответствующего полилинейного продолжения. В этом направлении недавно в [27, 28, 4, 29, 30, 31] получены некоторые важные результаты, а именно, построены выпуклые (вогнутые) продолжения булевых функций на множество $[0, 1]^n$ и изучены их свойства. Также на основе построенных выпуклых (вогнутых) продолжений булевых функций на $[0, 1]^n$, в частности, 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). Поэтому, несомненно, актуальным является построение вещественных продолжений булевых функций, представляющих интерес при преобразовании систем булевых уравнений к задаче непрерывной оптимизации, и изучение свойств таких вещественных продолжений булевых функций [4, 29].

Данная работа посвящается исследованию порядка гладкости наибольшего выпуклого продолжения на $[0, 1]^n$ произвольной булевой функции $f_B : \{0, 1\}^n \rightarrow \{0, 1\}$, недавно представленного в [28], а также является продолжением работ [13, 16, 26, 20, 25, 24, 27, 28, 4, 31]. В результате исследования установлен порядок дифференцируемости наибольшего выпуклого продолжения на $[0, 1]^n$ произвольной булевой функции $f_B : \{0, 1\}^n \rightarrow \{0, 1\}$, а именно, во-первых, оценивая наибольшее выпуклое продолжение на $[0, 1]^n$ произвольной булевой функции $f_B(x)$ с обеих сторон, аргументировано, что оно непрерывно на $[0, 1]^n$, а во-вторых, доказано, что если число существенных переменных булевой функции $f_B(x)$ меньше двух, то соответствующее наибольшее выпуклое продолжение является бесконечно дифференцируемым, а если оно не меньше двух, то соответствующее наибольшее выпуклое продолжение является лишь

непрерывным.

2. Используемые определения и обозначения

Пусть $\mathbb{B}^n = \{(b_1, b_2, \dots, b_n) : b_1, b_2, \dots, b_n \in \{0, 1\}\}$ — множество всевозможных двоичных слов (булевых векторов) длины n , $\mathbb{K}^n = \{(x_1, x_2, \dots, x_n) : x_1, x_2, \dots, x_n \in [0, 1]\}$ — n -мерный куб, натянутый на булевы векторы длины n .

Пусть $\text{int}(\mathbb{K}^n) = \{(x_1, x_2, \dots, x_n) : x_1, x_2, \dots, x_n \in (0, 1)\}$ — множество внутренних точек куба $\mathbb{K}^n$.

ОПРЕДЕЛЕНИЕ 1. *Отображение вида $f_B : \mathbb{B}^n \rightarrow \mathbb{B}$ называется булевой функцией.*

ОПРЕДЕЛЕНИЕ 2. *Переменная x_k , где $k \in \{1, 2, \dots, n\}$, булевой функции $f_B(x_1, x_2, \dots, x_n)$ называется существенной (булева функция $f_B(x_1, x_2, \dots, x_n)$ существенно зависит от x_k), если имеет место*

$$f_B(x_1, \dots, x_{k-1}, 0, x_{k+1}, \dots, x_n) \neq f_B(x_1, \dots, x_{k-1}, 1, x_{k+1}, \dots, x_n).$$

Пусть $\Lambda(x_1, x_2, \dots, x_n) = \left\{ (\lambda_{(0,0,\dots,0)}, \lambda_{(0,0,\dots,1)}, \dots, \lambda_{(1,1,\dots,1)}) \in \mathbb{K}^{2^n} : \right.$

$$\left. \sum_{(b_1, b_2, \dots, b_n) \in \mathbb{B}^n} \lambda_{(b_1, b_2, \dots, b_n)} \cdot (b_1, b_2, \dots, b_n, 1) = (x_1, x_2, \dots, x_n, 1) \right\}$$

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

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

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

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

- a) *отображение f_C на $\mathbb{K}^n$ является выпуклой функцией,*
- b) *имеет место равенство $f_C(b_1, b_2, \dots, b_n) = f_B(b_1, b_2, \dots, b_n) \quad \forall (b_1, b_2, \dots, b_n) \in \mathbb{B}^n$.*

ОПРЕДЕЛЕНИЕ 5. *Отображение вида $f_{NR} : \mathbb{K}^n \rightarrow \mathbb{R}$ назовём максимумом среди всех выпуклых продолжений на $\mathbb{K}^n$ булевой функции $f_B : \mathbb{B}^n \rightarrow \mathbb{B}$, если выполняются следующие два условия:*

- a) *отображение f_{NR} является выпуклым продолжением булевой функции f_B на $\mathbb{K}^n$,*
- b) *для любого f_C — выпуклого продолжения на $\mathbb{K}^n$ булевой функции f_B и любой $(x_1, x_2, \dots, x_n) \in \mathbb{K}^n$ справедливо $f_C(x_1, x_2, \dots, x_n) \leq f_{NR}(x_1, x_2, \dots, x_n)$.*

ЗАМЕЧАНИЕ 1. *Не теряя общности будем считать, что все переменные $x_1, x_2, \dots, x_n$ каждой булевой функции $f_B(x_1, x_2, \dots, x_n)$, рассматриваемой далее в работе, являются существенными.*

3. Установление порядка дифференцируемости максимального выпуклого продолжения на $[0, 1]^n$ произвольной булевой функции $f_B : \{0, 1\}^n \rightarrow \{0, 1\}$

В этом разделе сосредоточимся на изучении порядка дифференцируемости функции $f_{NR}(x_1, x_2, \dots, x_n)$, которая является максимумом среди всех выпуклых продолжений на $\mathbb{K}^n$ произвольной булевой функции $f_B(x_1, x_2, \dots, x_n)$, а именно, во-первых, аргументируем непрерывность функции $f_{NR}(x_1, x_2, \dots, x_n)$ на $\mathbb{K}^n$ для любого натурального n , а во-вторых, докажем, что если $n \geq 2$, то функция $f_{NR}(x_1, x_2, \dots, x_n)$ на $\mathbb{K}^n$ не дифференцируема, а если $n < 2$, то функция $f_{NR}(x_1, x_2, \dots, x_n)$ на $\mathbb{K}^n$ бесконечно дифференцируема.

Недавно в работе [28] доказано, что для произвольной булевой функции $f_B(x_1, x_2, \dots, x_n)$ соответствующая вещественная функция

$$f_{NR}(x_1, x_2, \dots, x_n) = \min_{\lambda \in \Lambda(x_1, x_2, \dots, x_n)} \left[\sum_{(b_1, b_2, \dots, b_n) \in \mathbb{B}^n} \lambda_{(b_1, b_2, \dots, b_n)} \cdot f_B(b_1, b_2, \dots, b_n) \right] \quad (1)$$

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

Начнём с обоснования непрерывности функции $f_{NR}(x_1, x_2, \dots, x_n)$ на $\mathbb{K}^n$.

ТЕОРЕМА 1. *Функция $f_{NR}(x_1, x_2, \dots, x_n)$, определённая формулой (1) на $\mathbb{K}^n$ непрерывна.*

ДОКАЗАТЕЛЬСТВО. Доказательство проведём индукцией по n .

i) Согласно следствиям 2 и 3, приведённым в [28] имеем, что, во-первых, для любой булевой функции $f_B(x)$, зависящей от одной переменной вещественная функция вида

$$f_{NR}(x) = (1 - x) \cdot f_B(0) + x \cdot f_B(1) \quad (2)$$

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

$$\begin{aligned} f_{NR}(x, y) &= (1 - x - y) \cdot f_B(0, 0) + x \cdot f_B(1, 0) + y \cdot f_B(0, 1) + \\ &+ \frac{f_B(0, 0) - f_B(0, 1) - f_B(1, 0) + f_B(1, 1)}{4} \cdot (2x + 2y - 1 - |x - y| + |x + y - 1|) + \\ &+ \frac{|f_B(0, 0) - f_B(0, 1) - f_B(1, 0) + f_B(1, 1)|}{4} \cdot (|x - y| + |x + y - 1| - 1) \end{aligned} \quad (3)$$

является единственным максимумом среди всех её выпуклых продолжений на $\mathbb{K}^2$. Следовательно, непрерывность функций $f_{NR}(x)$ и $f_{NR}(x, y)$, ввиду (2) и (3), очевидна.

ii) На основе базы *i)* предположим, что при $n = k$ для произвольной булевой функции $f_B(x_1, x_2, \dots, x_k)$ соответствующее наибольшее выпуклое продолжение $f_{NR}(x_1, x_2, \dots, x_k)$ непрерывно на $\mathbb{K}^k$.

iii) Основываясь на *i)* и *ii)* докажем, что функция $f_{NR}(x_1, x_2, \dots, x_{k+1})$, являющаяся максимумом среди всех выпуклых продолжений на $\mathbb{K}^{k+1}$ булевой функции $f_B(x_1, x_2, \dots, x_{k+1})$, непрерывна на $\mathbb{K}^{k+1}$. Пусть $(x_1^*, x_2^*, \dots, x_{k+1}^*)$ – произвольная точка куба $\mathbb{K}^{k+1}$. Для этого покажем, что имеет место равенство

$$\lim_{(\Delta x_1, \Delta x_2, \dots, \Delta x_{k+1}) \rightarrow (0, 0, \dots, 0)} f_{NR}(x_1^* + \Delta x_1, x_2^* + \Delta x_2, \dots, x_{k+1}^* + \Delta x_{k+1}) = f_{NR}(x_1^*, x_2^*, \dots, x_{k+1}^*). \quad (4)$$

С этой целью относительно $(x_1^*, x_2^*, \dots, x_{k+1}^*)$ рассмотрим два случая.

Случай 1. Пусть $(x_1^*, x_2^*, \dots, x_{k+1}^*) \in \text{int}(\mathbb{K}^{k+1})$. Ввиду близости точек, т. е. $(x_1^* + \Delta x_1, x_2^* + \Delta x_2, \dots, x_{k+1}^* + \Delta x_{k+1}) \rightarrow (x_1^*, x_2^*, \dots, x_{k+1}^*)$ и включения $(x_1^*, x_2^*, \dots, x_{k+1}^*) \in \text{int}(\mathbb{K}^{k+1})$ получим, что $(x_1^* + \Delta x_1, x_2^* + \Delta x_2, \dots, x_{k+1}^* + \Delta x_{k+1}) \in \text{int}(\mathbb{K}^{k+1})$. Из включений $x^* \in \text{int}(\mathbb{K}^{k+1})$ и

$(x^* + \Delta x) \in \text{int}(\mathbb{K}^{k+1})$, где $x^* = (x_1^*, x_2^*, \dots, x_{k+1}^*)$ и $\Delta x = (\Delta x_1, \Delta x_2, \dots, \Delta x_{k+1})$, следует, что существует $\delta > 0$ такое, что имеют место включения $x_L \in \text{int}(\mathbb{K}^{k+1})$ и $x^U \in \text{int}(\mathbb{K}^{k+1})$, где

$$x_L = x^* - \frac{\delta}{\|\Delta x\|} \cdot \Delta x \quad \text{и} \quad x^U = x^* + \Delta x + \frac{\delta}{\|\Delta x\|} \cdot \Delta x, \quad (5)$$

а также

$$\|\Delta x\| = \sqrt{(\Delta x_1)^2 + (\Delta x_2)^2 + \dots + (\Delta x_{k+1})^2}.$$

Из (5) получим

$$x^* = \frac{\|\Delta x\|}{\delta + \|\Delta x\|} \cdot x_L + \frac{\delta}{\delta + \|\Delta x\|} \cdot (x^* + \Delta x) \quad \text{и} \quad x^* + \Delta x = \frac{\|\Delta x\|}{\delta + \|\Delta x\|} \cdot x^U + \frac{\delta}{\delta + \|\Delta x\|} \cdot x^*. \quad (6)$$

Ввиду (6), выпуклости функции $f_{NR}(x)$ на $\mathbb{K}^{k+1}$ и неравенства Йенсена [32] имеем

$$\begin{aligned} f_{NR}(x^*) &\leq \frac{\|\Delta x\|}{\delta + \|\Delta x\|} \cdot f_{NR}(x_L) + \frac{\delta}{\delta + \|\Delta x\|} \cdot f_{NR}(x^* + \Delta x), \\ f_{NR}(x^* + \Delta x) &\leq \frac{\|\Delta x\|}{\delta + \|\Delta x\|} \cdot f_{NR}(x^U) + \frac{\delta}{\delta + \|\Delta x\|} \cdot f_{NR}(x^*). \end{aligned} \quad (7)$$

Из (7) получим

$$\frac{\|\Delta x\|}{\delta + \|\Delta x\|} \cdot (f_{NR}(x^U) - f_{NR}(x^*)) \geq f_{NR}(x^* + \Delta x) - f_{NR}(x^*) \geq \frac{\|\Delta x\|}{\delta} \cdot (f_{NR}(x^*) - f_{NR}(x_L)). \quad (8)$$

Из (1) следует, что $\forall n \in \mathbb{N}$ и $\forall x \in \mathbb{K}^n$ имеет место цепочка

$$\begin{aligned} 0 &= \min_{(\lambda_{(0,0,\dots,0)}, \dots, \lambda_{(1,1,\dots,1)}) \in \Lambda(x_1, x_2, \dots, x_n)} \left[\sum_{(b_1, b_2, \dots, b_n) \in \mathbb{B}^n} \lambda_{(b_1, b_2, \dots, b_n)} \cdot 0 \right] \leq f_{NR}(x) \leq \\ &\leq \min_{(\lambda_{(0,0,\dots,0)}, \dots, \lambda_{(1,1,\dots,1)}) \in \Lambda(x_1, x_2, \dots, x_n)} \left[\sum_{(b_1, b_2, \dots, b_n) \in \mathbb{B}^n} \lambda_{(b_1, b_2, \dots, b_n)} \cdot 1 \right] = 1. \end{aligned} \quad (9)$$

Из (8) и (9) следует, что справедлива цепочка неравенств

$$\frac{\|\Delta x\|}{\delta + \|\Delta x\|} \cdot (1 - f_{NR}(x^*)) \geq f_{NR}(x^* + \Delta x) - f_{NR}(x^*) \geq \frac{\|\Delta x\|}{\delta} \cdot (f_{NR}(x^*) - 1). \quad (10)$$

Теперь легко заметить, что справедливость (4) следует из цепочки (10).

Случай 2. Пусть $(x_1^*, x_2^*, \dots, x_{k+1}^*) \in \partial(\mathbb{K}^{k+1}) = \mathbb{K}^{k+1} \setminus \text{int}(\mathbb{K}^{k+1})$. Тогда существует $i \in \{1, 2, \dots, k+1\}$ такое, что справедливо включение $x_i^* \in \{0, 1\}$. Согласно ii), функции, полученные путем сужения, вида

$$\begin{aligned} &f_0(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1}) = \\ &= f_{NR}(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_{k+1}) = \min_{(\lambda_{(0,0,\dots,0)}, \dots, \lambda_{(1,1,\dots,1)}) \in \Lambda(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1})} \left[\sum_{(b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_{k+1}) \in \mathbb{B}^k} \lambda_{(b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_{k+1})} \cdot f_B(b_1, \dots, b_{i-1}, 0, b_{i+1}, \dots, b_{k+1}) \right] \end{aligned} \quad (11)$$

и

$$f_1(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1}) =$$

$$= f_{NR}(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_{k+1}) = \min_{(\lambda_{(0,0,\dots,0)}, \dots, \lambda_{(1,1,\dots,1)}) \in \Lambda(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1})} \left[\sum_{(b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_{k+1}) \in \mathbb{B}^k} \lambda_{(b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_{k+1})} \cdot f_B(b_1, \dots, b_{i-1}, 1, b_{i+1}, \dots, b_{k+1}) \right], \quad (12)$$

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

$$g(x_1, \dots, x_{k+1}) = \max(x_i, f_0(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1})) + \max(1 - x_i, f_1(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1})) - 1 \quad (13)$$

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

а) Имеет место равенство

$$g(b_1, \dots, b_{k+1}) = f_B(b_1, \dots, b_{k+1}) \quad \forall (b_1, \dots, b_{k+1}) \in \mathbb{B}^{k+1}.$$

б) Функция $g(x_1, \dots, x_{k+1})$ на $\mathbb{K}^{k+1}$ является выпуклой.

Обоснуем эти свойства:

а) Действительно, $\forall (b_1, \dots, b_{k+1}) \in \mathbb{B}^{k+1}$ имеем

$$\begin{aligned} g(b_1, \dots, b_{k+1}) &= \max(b_i, f_0(b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_{k+1})) + \max(1 - b_i, f_1(b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_{k+1})) - 1 = \\ &= (b_i \vee f_0(b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_{k+1})) + (\bar{b}_i \vee f_1(b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_{k+1})) - 1 = \\ &= (b_i \vee f_0(b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_{k+1})) \wedge (\bar{b}_i \vee f_1(b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_{k+1})) = \\ &= f_{b_i}(b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_{k+1}) = f_{NR}(b_1, \dots, b_{i-1}, b_i, b_{i+1}, \dots, b_{k+1}) = f_B(b_1, \dots, b_{k+1}). \end{aligned}$$

б) Функции $f_0(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1})$ и $f_1(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1})$, ввиду (11) и (12), на $\mathbb{K}^k$ являются выпуклыми и, следовательно, для любых $x, y \in \mathbb{K}^{k+1}$ и любого $\alpha \in [0, 1]$ имеем

$$\begin{aligned} g(\alpha \cdot x + (1 - \alpha) \cdot y) &= \max \left(\alpha x_i + (1 - \alpha) y_i, f_0(\alpha x_1 + (1 - \alpha) y_1, \dots, \alpha x_{i-1} + (1 - \alpha) y_{i-1}, \alpha x_{i+1} + \right. \\ &+ (1 - \alpha) y_{i+1}, \dots, \alpha x_{k+1} + (1 - \alpha) y_{k+1}) \left. \right) + \max \left(1 - (\alpha x_i + (1 - \alpha) y_i), f_1(\alpha x_1 + (1 - \alpha) y_1, \dots, \alpha x_{i-1} + \right. \\ &+ (1 - \alpha) y_{i-1}, \alpha x_{i+1} + (1 - \alpha) y_{i+1}, \dots, \alpha x_{k+1} + (1 - \alpha) y_{k+1}) \left. \right) - 1 \leq \max \left(\alpha x_i + (1 - \alpha) y_i, \alpha \cdot f_0(x_1, \right. \\ &\dots, x_{i-1}, x_{i+1}, \dots, x_{k+1}) + (1 - \alpha) \cdot f_0(y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_{k+1}) \left. \right) + \max \left(\alpha(1 - x_i) + (1 - \alpha)(1 - y_i), \right. \\ &\alpha \cdot f_1(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1}) + (1 - \alpha) \cdot f_1(y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_{k+1}) \left. \right) - 1 \leq \\ &\leq \alpha \cdot \max(x_i, f_0(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1})) + (1 - \alpha) \cdot \max(y_i, f_0(y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_{k+1})) + \\ &+ \alpha \cdot \max(1 - x_i, f_1(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1})) + (1 - \alpha) \cdot \max(1 - y_i, f_1(y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_{k+1})) - 1 = \\ &= \alpha \cdot g(x) + (1 - \alpha) \cdot g(y). \end{aligned}$$

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

$$f_{NR}(x^* + \Delta x) - f_{NR}(x^*) \geq g(x^* + \Delta x) - f_{NR}(x^*), \quad (14)$$

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

$$f_{NR}(x^* + \Delta x) - f_{NR}(x^*) =$$

$$\begin{aligned}
& f_{NR}\left((1 - (1 - 2x_i^*)\Delta x_i) \cdot (x_1^* + \Delta x_1, \dots, x_{i-1}^* + \Delta x_{i-1}, x_i^*, x_{i+1}^* + \Delta x_{i+1}, \dots, x_{k+1}^*) + \right. \\
& \left. + (1 - 2x_i^*)\Delta x_i \cdot (x_1^* + \Delta x_1, \dots, x_{i-1}^* + \Delta x_{i-1}, 1 - x_i^*, x_{i+1}^* + \Delta x_{i+1}, \dots, x_{k+1}^*)\right) - f_{NR}(x^*) \leq \\
& \leq (1 - (1 - 2x_i^*)\Delta x_i) \cdot f_{NR}(x_1^* + \Delta x_1, \dots, x_{i-1}^* + \Delta x_{i-1}, x_i^*, x_{i+1}^* + \Delta x_{i+1}, \dots, x_{k+1}^*) + \\
& + (1 - 2x_i^*)\Delta x_i \cdot f_{NR}(x_1^* + \Delta x_1, \dots, x_{i-1}^* + \Delta x_{i-1}, 1 - x_i^*, x_{i+1}^* + \Delta x_{i+1}, \dots, x_{k+1}^*) - f_{NR}(x^*). \quad (15)
\end{aligned}$$

Итак, ввиду (13) 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 (14) и (15) при $(\Delta x_1, \Delta x_2, \dots, \Delta x_{k+1}) \rightarrow (0, 0, \dots, 0)$, получим (4). Теорема 1 полностью доказана. $\square$

Далее сформулируем теорему, утверждающую, что если $n \geq 2$, то функция $f_{NR}(x)$, являющаяся максимумом среди всех выпуклых продолжений на $\mathbb{K}^n$ булевой функции $f_B(x)$, не дифференцируема на $\mathbb{K}^n$.

ТЕОРЕМА 2. *Если n , что является числом существенных переменных произвольной булевой функции $f_B(x_1, x_2, \dots, x_n)$, не менее двух, то вещественная функция $f_{NR}(x_1, x_2, \dots, x_n)$, являющаяся максимумом среди всех выпуклых продолжений на $\mathbb{K}^n$ булевой функции $f_B(x_1, x_2, \dots, x_n)$, не является дифференцируемой на $\mathbb{K}^n$.*

ДОКАЗАТЕЛЬСТВО. Докажем от противного: пусть вещественная функция $f_{NR}(x_1, x_2, \dots, x_n)$, которая является максимумом среди всех выпуклых продолжений на $\mathbb{K}^n$ булевой функции $f_B(x_1, x_2, \dots, x_n)$, является дифференцируемой в каждой точке $(x_1^*, x_2^*, \dots, x_n^*)$ куба $\mathbb{K}^n$ при $n \geq 2$. Тогда имеем, что $\forall (b_3, \dots, b_n) \in \mathbb{B}^{n-2}$ суженная вещественная функция $f_{NR}(x_1, x_2, b_3, \dots, b_n)$ является дифференцируемой в каждой точке (x_1^*, x_2^*) квадрата $\mathbb{K}^2$. Нетрудно проверить, что в силу того, что булева функция $f_B(x_1, x_2, \dots, x_n)$ существенно зависит от всех своих переменных, у нее имеется выделяемая пара переменных, которые без ограничения общности можно считать равными x_1 и x_2 , т.е. существует $(b_3^*, \dots, b_n^*) \in \mathbb{B}^{n-2}$ такой, что переменные x_1 и x_2 для суженной булевой функции $f_B(x_1, x_2, b_3^*, \dots, b_n^*)$ являются существенными. Отсюда получим, что вещественная функция вида $g_{NR}(x_1, x_2) = f_{NR}(x_1, x_2, b_3^*, \dots, b_n^*)$, которая является максимумом среди всех выпуклых продолжений на $\mathbb{K}^2$ булевой функции $g_B(x_1, x_2) = f_B(x_1, x_2, b_3^*, \dots, b_n^*)$, является дифференцируемой в каждой точке (x_1^*, x_2^*) квадрата $\mathbb{K}^2$. Хорошо известно, что переменные x_1 и x_2 являются существенными для булевой функции $g_B(x_1, x_2)$ тогда и только тогда, когда справедливо включение

$$\begin{aligned}
& (g_B(0, 0), g_B(0, 1), g_B(1, 0), g_B(1, 1)) \in \{(0, 0, 0, 1), (0, 0, 1, 0), (0, 1, 0, 0), \\
& (0, 1, 1, 0), (0, 1, 1, 1), (1, 0, 0, 0), (1, 0, 0, 1), (1, 0, 1, 1), (1, 1, 0, 1), (1, 1, 1, 0)\}. \quad (16)
\end{aligned}$$

Теперь, с одной стороны, ввиду включения (16), получаем, что

$$g_B(0, 0) - g_B(0, 1) - g_B(1, 0) + g_B(1, 1) \neq 0, \quad (17)$$

а с другой стороны, ввиду (3), имеем, что

$$\begin{aligned}
& g_{NR}(x_1, x_2) = (1 - x_1 - x_2) \cdot g_B(0, 0) + x_1 \cdot g_B(1, 0) + x_2 \cdot g_B(0, 1) + \\
& + \frac{g_B(0, 0) - g_B(0, 1) - g_B(1, 0) + g_B(1, 1)}{4} \cdot (2x_1 + 2x_2 - 1 - |x_1 - x_2| + |x_1 + x_2 - 1|) + \\
& + \frac{|g_B(0, 0) - g_B(0, 1) - g_B(1, 0) + g_B(1, 1)|}{4} \cdot (|x_1 - x_2| + |x_1 + x_2 - 1| - 1). \quad (18)
\end{aligned}$$

В силу (17) из (18) следует, что функция $g_{NR}(x_1, x_2)$ не является дифференцируемой на $\mathbb{K}^2$, т.е. не является дифференцируемой в каждой точке (x_1^*, x_2^*) квадрата $\mathbb{K}^2$. Возникшее противоречие завершает доказательство теоремы 2. $\square$

4. Заключение

Итак, ввиду формулы (2) и теорем 1, 2 имеем, что если $n \geq 2$, то функция $f_{NR}(x_1, x_2, \dots, x_n)$, являющаяся максимумом среди всех выпуклых продолжений на $\mathbb{K}^n$ произвольной булевой функции $f_B(x_1, x_2, \dots, x_n)$, непрерывна на $\mathbb{K}^n$, но не дифференцируема на $\mathbb{K}^n$, а если $n < 2$, то функция $f_{NR}(x_1, x_2, \dots, x_n)$, являющаяся максимумом среди всех выпуклых продолжений на $\mathbb{K}^n$ произвольной булевой функции $f_B(x_1, x_2, \dots, x_n)$, линейна и, следовательно, бесконечно дифференцируема на $\mathbb{K}^n$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Brown F. M. Boolean Reasoning: The logic of Boolean Equations. Kluwer Academic Publishers, Boston, 1990.
2. Баротов, Д. Н., Баротов, Р. Н. Об одном приведении системы булевых уравнений к эквивалентной системе полиномиальных уравнений // Математические структуры и моделирование. 2024. № 1(69). С. 5–17. doi: 10.24147/2222-8772.2024.1.5-17.
3. Hammer, P. L., Rudeanu, S. Boolean Methods in Operations Research and Related Areas. Springer Verlag, Berlin, 1968.
4. Баротов, Д. Н., Баротов, Р. Н. Конструирование гладких выпуклых продолжений булевых функций // Вестник российских университетов. Математика. 2024. Т. 29. № 145. С. 20–28. doi:10.20310/2686-9667-2024-29-145-20-28.
5. Bard, G. V. Algorithms for solving linear and polynomial systems of equations over finite fields, with applications to cryptanalysis. University of Maryland, College Park, 2007.
6. Faugere, J. C., Joux, A. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Grobner bases // Annual International Cryptology Conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003. P. 44–60.
7. Armknecht, F. Improving fast algebraic attacks // Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers 11. Springer Berlin Heidelberg, 2004. P. 65–82.
8. Bardet, M., Faugere, J. C., Salvy, B., Spaenlehauer, P. J. On the complexity of solving quadratic Boolean systems // Journal of Complexity. 2013. Vol. 29. no. 1. P. 53–75. doi: 10.1016/j.jco.2012.07.001.
9. Courtois, N. T. Fast algebraic attacks on stream ciphers with linear feedback // Advances in Cryptology-CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003. Proceedings 23. Springer Berlin Heidelberg, 2003. P. 176–194.
10. Liu, M., Lin, D., Pei, D. Fast algebraic attacks and decomposition of symmetric Boolean functions // IEEE Transactions on Information Theory. 2011. Vol. 57. no. 7. P. 4817–4821. doi: 10.1109/TIT.2011.2145690.
11. Gu, J. How to Solve Very Large-Scale Satisfiability (VLSS) Problems // Technical Report UCECETR-90-002, University of Calgary: Calgary, 1990.
12. Gu, J. On optimizing a search problem // Artificial Intelligence Methods and Applications. 1992. P. 63–105. doi: 10.1142/9789814354707_0002.

13. Баротов, Д. Н., Музафаров, Д. З., Баротов, Р. Н. Об одном методе решения систем булевых алгебраических уравнений // Современная математика и концепции инновационного математического образования. 2021. Т. 8, № 1. С. 17–23.
14. Gu, J. Global optimization for satisfiability (SAT) problem // IEEE Transactions on Knowledge and Data Engineering. 1994. Vol. 6. no. 3. P. 361–381. doi: 10.1109/69.334864.
15. Gu, J., Gu, Q., Du, D. On optimizing the satisfiability (SAT) problem // Journal of Computer Science and Technology. 1999. Vol. 14. no. 1. P. 1–17. doi: 10.1007/BF02952482.
16. Transformation method for solving system of Boolean algebraic equations / Barotov, D., Osipov, A., Korchagin, S., Pleshakova, E., Muzafarov, D., Barotov, R., Serdechnyy, D. // Mathematics. 2021. Vol. 9, 3299. doi: 10.3390/math9243299.
17. Converting of Boolean Expression to Linear Equations, Inequalities and QUBO Penalties for Cryptanalysis / Pakhomchik, A. I., Voloshinov, V. V., Vinokur, V. M., Lesovik, G. B. // Algorithms. 2022. Vol. 15, 33. doi: 10.3390/a15020033.
18. Algebraic attacks on block ciphers using quantum annealing / Burek, E., Wronski, M., Mank, K., Misztal, M. // IEEE Transactions on Emerging Topics in Computing. 2022. Vol. 10. no. 2. P. 678–689. doi: 10.1109/TETC.2022.3143152.
19. Abdel-Gawad, A. H., Atiya, A. F., Darwish, N. M. Solution of systems of Boolean equations via the integer domain // Information Sciences. 2010. Vol. 180, no. 2, P. 288–300. doi: 10.1016/j.ins.2009.09.010.
20. The Development of Suitable Inequalities and Their Application to Systems of Logical Equations / Barotov, D. N., Barotov, R. N., Soloviev, V., Feklin, V., Muzafarov, D., Ergashboev, T., Egamov, K. // Mathematics. 2022. Vol. 10, 1851. doi: 10.3390/math10111851.
21. Faugere, J. C. A new efficient algorithm for computing Grobner bases (F4) // Journal of pure and applied algebra. 1999. Vol. 139. no. 1-3. P. 61–88. doi: 10.1016/S0022-4049(99)00005-5.
22. Faugere, J. C. A new efficient algorithm for computing Grobner bases without reduction to zero (F5) // Proceedings of the 2002 international symposium on Symbolic and algebraic computation. 2002. P. 75–83.
23. 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.
24. Баротов, Д. Н., Баротов, Р. Н. Полилинейные продолжения некоторых дискретных функций и алгоритм их нахождения // Вычислительные методы и программирование. 2023. Т. 24. С. 10–23. doi: 10.26089/NumMet.v24r102.
25. Barotov, D. N. Target Function without Local Minimum for Systems of Logical Equations with a Unique Solution // Mathematics. 2022. Vol. 10, 2097. doi: 10.3390/math10122097.
26. Barotov, D. N., Barotov, R. N. Polylinear Transformation Method for Solving Systems of Logical Equations // Mathematics. 2022. Vol. 10, 918. doi: 10.3390/math10060918.
27. Баротов, Д. Н. Выпуклое продолжение булевой функции и его приложения // Дискретный анализ и исследование операций. 2024. Т. 31, № 1. С. 5–18. doi: 10.33048/daio.2024.31.779.
28. Баротов, Д. Н. О существовании и свойствах выпуклых продолжений булевых функций // Матем. заметки. 2024. Т. 115, № 4. С. 533–551. doi: 10.4213/mzm14105.

29. 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. doi: 10.20948/prepr-2024-30.
30. Баротов, Д. Н. Вогнутые продолжения булевых функций и некоторые их свойства и приложения // Известия Иркутского государственного университета. Серия «Математика». 2024. Т. 49. С. 105–123. doi: 10.26516/1997-7670.2024.49.105.
31. Баротов, Д. Н. Выпуклые продолжения некоторых дискретных функций // Дискретный анализ и исследование операций. 2024. Т. 31, № 3. С. 5–23. doi: 10.33048/daio.2024.31.789.
32. Jensen, J. L. W. V. Sur les fonctions convexes et les inegalites entre les valeurs moyennes // Acta mathematica. 1906. Vol. 30. no. 1. P. 175–193. doi: 10.1007/BF02418571.

REFERENCES

1. Brown, F.M. 1990, *Boolean Reasoning: The logic of Boolean Equations*, Boston: Kluwer Academic Publishers.
2. Barotov, D.N. & Barotov, R.N. 2024, “On a reduction of the system of Boolean equations to an equivalent system of polynomial equations”, *Mathematical Structures and Modeling*, no. 1(69), pp. 5–17. doi: 10.24147/2222-8772.2024.1.5-17.
3. Hammer, P.L. & Rudeanu, S. 1968, *Boolean Methods in Operations Research and Related Areas*, Berlin: Springer Verlag.
4. Barotov, D.N. & Barotov, R.N. 2024, “Construction of smooth convex extensions of Boolean functions”, *Russian Universities Reports. Mathematics*, vol. 29, no. 145, pp. 20–28. doi:10.20310/2686-9667-2024-29-145-20-28.
5. Bard, G.V. 2007, *Algorithms for solving linear and polynomial systems of equations over finite fields, with applications to cryptanalysis*, College Park: University of Maryland.
6. Faugere, J.C. & Joux, A. 2003, “Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Grobner bases”, in *Annual International Cryptology Conference*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 44–60.
7. Armknecht, F. 2004, “Improving fast algebraic attacks”, in *Fast Software Encryption: 11-th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers 11*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 65–82.
8. Bardet, M., Faugere, J.C., Salvye, B. & Spaenlehauer, P.J. 2013, “On the complexity of solving quadratic Boolean systems”, *Journal of Complexity*, vol. 29, no. 1, pp. 53–75. doi:10.1016/j.jco.2012.07.001.
9. Courtois, N.T. 2003, “Fast algebraic attacks on stream ciphers with linear feedback”, in *Advances in Cryptology-CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003. Proceedings 23*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 176–194.
10. Liu, M., Lin, D. & Pei, D. 2011, “Fast algebraic attacks and decomposition of symmetric Boolean functions”, *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4817–4821. doi:10.1109/TIT.2011.2145690.

11. Gu, J. 1990, “How to Solve Very Large-Scale Satisfiability (VLSS) Problems”, Technical Report UCECETR-90-002, University of Calgary, Calgary.
12. Gu, J. 1992, “On optimizing a search problem”, *Artificial Intelligence Methods and Applications*, pp. 63–105. doi:10.1142/9789814354707_0002.
13. Barotov, D.N., Muzafarov, D.Z. & Barotov, R.N. 2021, “On one method for solving systems of Boolean algebraic equations”, *Mod. Math. Concept Innov. Math. Educ.*, vol. 8, pp. 17–23.
14. Gu, J. 1994, “Global optimization for satisfiability (SAT) problem”, *IEEE Transactions on Knowledge and Data Engineering*, vol. 6, no. 3, pp. 361–381. doi:10.1109/69.334864.
15. Gu, J., Gu, Q. & Du, D. 1999, “On optimizing the satisfiability (SAT) problem”, *Journal of Computer Science and Technology*, vol. 14, no. 1, pp. 1–17. doi:10.1007/BF02952482.
16. Barotov, D., Osipov, A., Korchagin, S., Pleshakova, E., Muzafarov, D., Barotov, R. & Serdechnyy, D. 2021, “Transformation method for solving system of Boolean algebraic equations”, *Mathematics*, vol. 9, p. 3299. doi:10.3390/math9243299.
17. Pakhomchik, A.I., Voloshinov, V.V., Vinokur, V.M. & Lesovik, G.B. 2022, “Converting of Boolean Expression to Linear Equations, Inequalities and QUBO Penalties for Cryptanalysis”, *Algorithms*, vol. 15, p. 33. doi:10.3390/a15020033.
18. Burek, E., Wronski, M., Mank, K. & Misztal, M. 2022, “Algebraic attacks on block ciphers using quantum annealing”, *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 2, pp. 678–689. doi:10.1109/TETC.2022.3143152.
19. Abdel-Gawad, A.H., Atiya, A.F. & Darwish, N.M. 2010, “Solution of systems of Boolean equations via the integer domain”, *Information Sciences*, vol. 180, no. 2, pp. 288–300. doi:10.1016/j.ins.2009.09.010.
20. Barotov, D.N., Barotov, R.N., Soloviev, V., Feklin, V., Muzafarov, D., Ergashboev, T. & Egamov, K. 2022, “The Development of Suitable Inequalities and Their Application to Systems of Logical Equations”, *Mathematics*, vol. 10, p. 1851. doi:10.3390/math10111851.
21. Faugere, J.C. 1999, “A new efficient algorithm for computing Grobner bases (F4)”, *Journal of Pure and Applied Algebra*, vol. 139, no. 1-3, pp. 61–88. doi:10.1016/S0022-4049(99)00005-5.
22. Faugere, J.C. 2002, “A new efficient algorithm for computing Grobner bases without reduction to zero (F5)”, *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pp. 75–83.
23. Faizullin, R.T., Dul’keit, V.I. & Ogorodnikov, Yu.Yu. 2013, “A hybrid search method for the approximate solution of the 3-satisfiability problem associated with the factorization problem”, *Trudy Instituta Matematiki i Mekhaniki*, vol. 19, no. 2, pp. 285–294.
24. Barotov, D.N. & Barotov, R.N. 2023, “Polylinear continuations of some discrete functions and an algorithm for finding them”, *Numerical Methods and Programming (Vychislitel’nye Metody i Programirovanie)*, vol. 24, pp. 10–23. doi:10.26089/NumMet.v24r102.
25. Barotov, D.N. 2022, “Target Function without Local Minimum for Systems of Logical Equations with a Unique Solution”, *Mathematics*, vol. 10, p. 2097. doi:10.3390/math10122097.
26. Barotov, D.N. & Barotov, R.N. 2022, “Polylinear Transformation Method for Solving Systems of Logical Equations”, *Mathematics*, vol. 10, p. 918. doi:10.3390/math10060918.

27. Barotov, D.N. 2024, “Convex Continuation of a Boolean Function and Its Applications”, *Journal of Applied and Industrial Mathematics*, vol. 18, pp. 1–9. doi:10.1134/S1990478924010010.
28. Barotov, D.N. 2024, “On the Existence and Properties of Convex Extensions of Boolean Functions”, *Mathematical Notes*, vol. 115, no. 4, pp. 489–505. doi:10.1134/S0001434624030210.
29. Barotov, D.N. & Sudakov, V.A. 2024, “On inequalities between convex, concave, and polylinear continuations of Boolean functions”, *Preprints of the M.V. Keldysh Institute of Applied Mathematics*, no. 30, pp. 1–13. doi:10.20948/prepr-2024-30.
30. Barotov, D.N. 2024, “Concave Continuations of Boolean Functions and Some of Their Properties and Applications”, *The Bulletin of Irkutsk State University. Series Mathematics*, vol. 49, pp. 105–123. (in Russian). doi:10.26516/1997-7670.2024.49.105.
31. Barotov, D.N. 2024, “Convex Continuations of Some Discrete Functions”, *Journal of Applied and Industrial Mathematics*, vol. 18, no. 3, pp. 412–423. doi:10.1134/S1990478924030049.
32. Jensen, J.L.W.V. 1906, “Sur les fonctions convexes et les inégalités entre les valeurs moyennes”, *Acta Mathematica*, vol. 30, no. 1, pp. 175–193. doi:10.1007/BF02418571.

Получено: 25.01.2025

Принято в печать: 27.08.2025